А.М. ГОЛИКОВ

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ. ЧАСТЬ 2.

Учебное пособие

для специалитета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации)

Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу

Томск 2018

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
Томский государственный университет систем управления и
радиоэлектроники

А.М. ГОЛИКОВ

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ.

ЧАСТЬ 2.

Учебное пособие

для специалитета: 11.05.01 - Радиоэлектронные системы и комплексы
(Радиоэлектронные системы передачи информации)

Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу

Томск 2018

УДК 621.39(075.8)
ББК 32.973(я73)
Г 60

Голиков А.М.

Голиков, А. М. Защита информации в радиоэлектронных системах передачи информации. Часть 2. Защита от утечки информации по техническим каналам: Учебное пособие для специалитета 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2018. — 264 с. — Режим доступа: https://edu.tusur.ru/publications/8860

Учебное пособие является учебно-методическим комплексом дисциплины (УМКД) специалитета: 11.05.01 - Радиоэлектронные системы и комплексы (Радиоэлектронные системы передачи информации). Учебное пособие содержит лекционный материал, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу по курсу «Защита информации в радиоэлектронных системах передачи информации».

. В учебном пособии рассмотрены технические методы и средства защиты информации, даны понятия об объектах защиты информации, о характеристиках угроз, технических каналах утечки информации, методах и средствах поиска электронных устройств перехвата информации, освещаются вопросы организации инженерно-технической защиты информации и ее методическое обеспечение.

СОДЕРЖАНИЕ

Глава 1. Объекты информационной защиты

1.1. Понятие о конфиденциальной информации

В соответствии с терминологией закона “Об информации, информатизации и защите информации” информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. По Ожегову С.И. сведения - это знания. Следовательно, в общем случае информация - это знания в самом широком понимании этого слова. Не только образовательные или научные знания, а любые сведения и данные, которые присутствуют в любом объекте и необходимы для функционирования любых информационных систем (живых существ или созданных человеком). Так как информация отражает свойства материальных объектов и отношения между ними, то ее можно отнести к объектам познания, а защищаемую информацию - предметом защиты.

Защите подлежит секретная и конфиденциальная информация. К секретной относится информация, содержащая государственную тайну. Ее несанкционированное распространение может нанести ущерб интересам государственным органам, организациям и РФ в целом. Под конфиденциальной понимается информация, содержащую коммерческую и иную тайну.

Информация как предмет познания имеет ряд особенностей:

- она нематериальна в том смысле, что не удается измерить известными физическими методами и приборами ее массу, размеры, энергию;

-информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи;

- информация о самом себе содержится в любом материальном объекте;

- без информации не может существовать жизнь в любой форме и не могут функционировать созданные человеком любые информационные системы.

Без информации 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) по своим последствиям не менее разрушителен, чем голод физический. Несмотря на определенные достижения прикладной области науки - информатики, занимающейся информационными процессами, достаточно четкого понимания сущности информации наука пока не имеет.

1.1.1. Основные свойства информации как предмета защиты

С точки зрения защиты информация обладает рядом свойств, основными 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 информационной 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 перемещения и вида носителя. В принципе информация может быть передана на любое расстояние сколь угодно малой энергией . Это обстоятельство не учитывается при обосновании утверждений о невозможности непосредственной передачи информации между людьми на большие расстояния из-за энергетических ограничений.

2. Ценность информации оценивается степенью полезности ее для владельца (получателя). Она может обеспечивать ее владельцу определенные преимущества, приносить прибыль, уменьшить риск в его деятельности в результате принятия более обоснованных решений.

Нейтральная информация не влияет на состояние дел ее получателя, 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 получателя - пользователя. Под пользователями подразумевается как один человек или автомат, так и группа людей и даже все человечество. Поэтому при защите информации важно среди других задач защиты, прежде всего, определяют круг лиц (фирм, государств), заинтересованных в защищаемой информации, так как вероятно, что среди них окажутся злоумышленники.

3. Учитывая, что информация может быть для получателя полезной или вредной, т.е. приносить ему прибыль или ущерб, 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 результаты, 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 его научно-исследовательской деятельности, заимствована из различных легальных 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 или аналитических центрах, группах и т. д.;
- покупки информации на рынке информации;
- добывания информации противоправными действиями.

Прибыль от информации в виду 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 и более качественнее должна быть информация. Размышления перед принятием решения 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.

Недостаток времени на ее обработку по последствиям идентичен недостатку информации в виде и форме, которые необходимы при принятии конкретного решения. Поэтому многочисленные помощники государственных деятелей готовят им информацию в сжатом виде, которые позволяют этим лицам принять обоснованные решения за короткое время.

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. В зависимости от вида информации ее ценность может меняться в значительных пределах. Как правило, ценность информации со временем снижается, но бывают исключения. 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 ядерной энергии.

Уменьшение ценности информации во времени называют ее старением. Старение информации $C_и$ во времени в первом приближении можно аппроксимировать выражением вида:

$$C_И(\tau) \approx C_0 \exp(-2.3\tau / \tau_{жц}),$$

где C_0 - полезность информации в момент ее возникновения (создания);

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

$\tau_{жц}$ - 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 следующие 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. Учитывая конкретность полезности информации, нельзя объективно (без учета ее потребителя) оценить количество и качество информации. В теории информации предложен энтропийный подход, В соответствии с ним количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) в выборе или ожидания событий после получения информации. Количество информации тем больше, чем ниже вероятность события. Такой подход хорошо разработан для определения количества информации, передаваемой 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:

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

где P_i — 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 как от содержания сообщения, так и от приращения информации у ее получателя. Количество информации, определяемое по этой формуле, одинаковое при передаче бессмысленного текста или сообщения о жизненно важных для получателя сведений. 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 сложную 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 ее 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 новых знаний - тезаурус получателя не пополняется, во втором - получатель не понимает смысл сообщения и не может установить отношения с другими элементами тезауруса. Подобное происходит, когда совершаются «преждевременные» научные открытия, которые даже для научной общественности являются “вещью в себе”. В истории науки и искусства много фактов оторжения общественностью идей и произведений, опережающих “свое время”. Например, доклад русского математика Н. И. Лобачевского на заседании физико-математического факультета Казанского университета в 1826 г. с изложением основ созданной им неевклидовой геометрии, которые рассматриваются в настоящее время как крупнейшее достижение математической мысли в истории мировой науки, почти никем не был понят и подвергся резкой критике.

Аналогичная ситуация с качеством информации. Качество информации характеризуется ее полезностью. Чрезвычайно ценная информация для одних владельцев или потребителей может не представлять ценности для других. Даже информация, ценная для всего человечества, например, технология изготовления лекарств от опасных болезней, для отдельного здорового человека она может не представлять интерес.

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 изучения литературных источников (самообучения), приглашения на работу более знающего специалиста, направления на учебу своих сотрудников, покупку патента или лицензии. Приобретение знаний путем хищения является незаконным способом увеличения тезауруса.

В природе и обществе наблюдается процессы как увеличения тезауруса владельца в результате синтеза информации, так и выравнивания тезаурусов разных владельцев. Выравнивание тезаурусов происходит путем передачи информации от тезауруса большего объема тезаурусу меньшего объема. Кроме целенаправленной (законной или незаконной) деятельности по передаче информации имеют место случайные процессы выравнивания тезаурусов владельцев, аналогично выравниванию температуры в замкнутом пространстве. Этот процесс объективно проявляется в любой организации и государстве путем случайных, трудно контролируемых процессов распространения информации от источника с большим объемом тезауруса к получателю, в том числе несанкционированному, с меньшим объемом тезауруса. Необходимы большие затраты и усилия для замедления процессов выравнивания тезаурусов, так же как, например, трудно удержать сгусток энергии от растекания.

При выравнивании тезаурусов коммерческая цена информации убывает, а ценность

информации может как возрастать, так и убывает. Действительно, закон Ома знают очень много людей, но от этого полезность его для практики не уменьшается. Но покупателя на него вряд ли удастся найти, так как изучение закона Ома входит в программу обязательного школьного образования.

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.

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 и военную тайну. В соответствии с постановлением Правительства РФ №870 от 4 сентября 1995 г. информации секретной, совершенно секретной и особой важности относится информация, несанкционированное распространение которой может нанести ущерб соответственно государственной организации (предприятию, учреждениею), отрасли (ведомству, министерству) и РФ в целом. Для несекретной конфиденциальной информации вводят гриф “для служебного пользования”.

Для обозначения конфиденциальности коммерческой и личной 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”. Предлагается также двухуровневая шкала ранжирования коммерческой информации: “коммерческая тайна” и “ для служебного пользования”.

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

- величина наносимого экономического и морального ущерба организации;
- реальность создания предпосылок для катастрофических последствий в деятельности организации (предприятия), в том числе для банкротства.

1.1.2. Виды защищаемой информации

По содержанию любая информация относится к семантической (в переводе с латинского - содержащей смысл) и к информации о признаках 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) 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 создается 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. Делаются попытки дополнить эти каналы воздействием на органы обоняния человека путем создания соответствующих запахов. 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 находится конфиденциальная информация. В зависимости от вида описания объекта признаковая информация делится на информацию о его внешнем виде (видовых признаках), о его полях (сигнальных признаках), о структуре и составе его веществ (вещественных признаках). Классификация информации по содержанию представлена на рис. 1. 1.

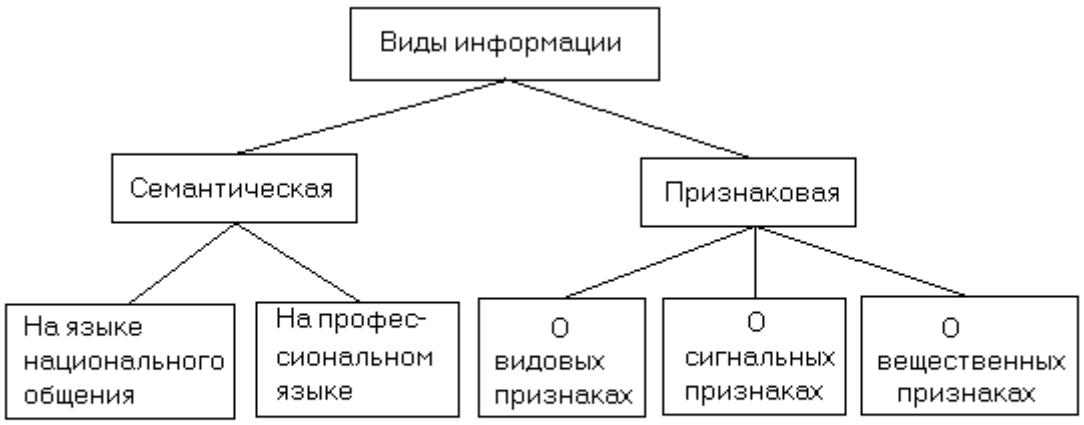


Рис. 1. 1. Классификация информации, защищаемой техническими средствами.

Защищаемая информация неоднородна по содержанию, объему и ценности. Следовательно, защита будет рациональной в том случае, когда уровень защиты, а, следовательно, затраты, соответствуют количеству и качеству информации. Если затраты на защиту информации выше ее цены, то уровень защиты неоправданно велик, если существенно меньше, то возможно уничтожение, хищение или модернизация

информации, приводящие к значительному ущербу. Для обеспечения рациональной защиты возникает необходимость структурирования конфиденциальной информации, т. е. разделения ее на так называемые информационные элементы.

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

- имеет конкретный источник информации (документ, человек, образец продукции и т. д.);
- содержится на отдельном носителе;
- имеет определенную ценность.

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.

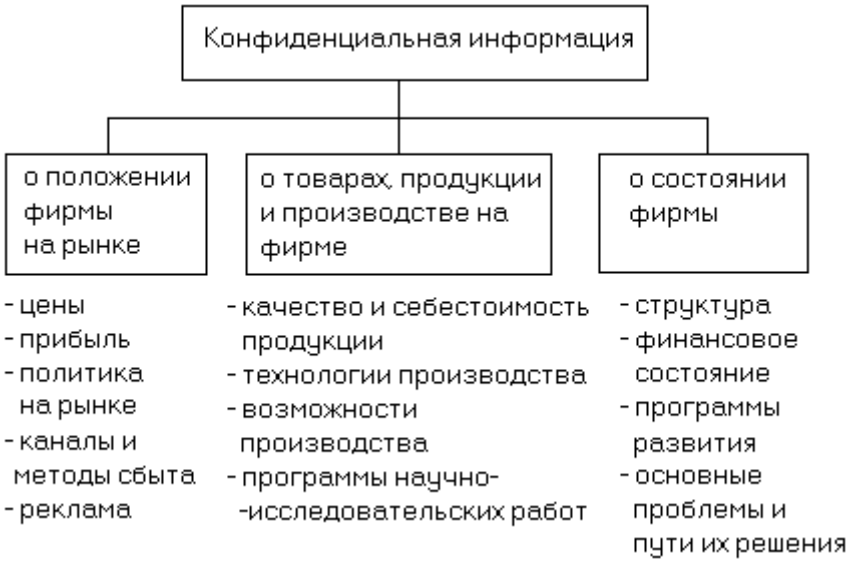


Рис. 1.2. Типовая структура конфиденциальной информации

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

Перечень сведений, составляющих коммерческую тайну (на рис. 1.2 - конфиденциальная информация), соответствует нулевому (исходному) уровню иерархии структуры. Эта информация на 1-м уровне разделяется на 3 группы, каждая из которых соответствует темам: "положение фирмы на рынке", "деятельность фирмы", "состояние фирмы". Тематика "цены", "прибыль" и т. д. объединяет информацию 2-го уровня. Далее на 3-м уровне детализируются сведения, относящиеся к темам “цены”, “ прибыль”, “ качество и себестоимость продукции” и т. д. до сведений, которые содержатся у конкретного источника информации. Такая информация является структурированной.

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

1.2. Демаскирующие признаки объектов защиты

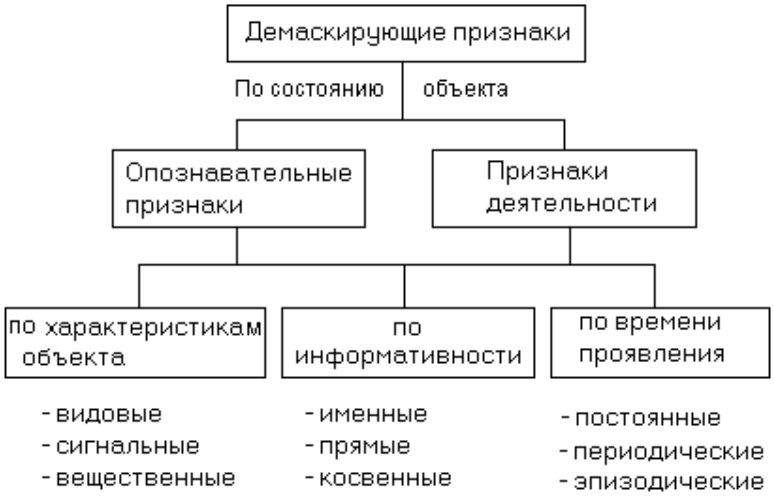
Задача защиты признаковой информации решается, прежде всего, путем предотвращения обнаружения и распознавания объектов, содержащих эти признаки. Среди множества признаков, присущих конкретному объекту, существуют признаки,

которые позволяют обнаруживать его среди других похожих объектов и распознать его принадлежность, назначение, функции, свойства, особенности и характеристики.

Признаки, позволяющие отличить один объект от другого, называются демаскирующими. Демаскирующие признаки объекта составляют часть его признаков, а значения их отличаются от значений соответствующих признаков других объектов. Совпадающие значения признаков не относятся к демаскирующим. Например, признак “рост человека” без указания его значения не является демаскирующим, так как он относится ко всем людям.

1 .2.1 Классификация демаскирующих признаков

Классификация признаков по различным основаниям дана на рис. 1.3.



1.3. Классификация демаскирующих признаков

Демаскирующие признаки объекта описывают его различные состояния, характеристики и свойства.

По состоянию объектов демаскирующие признаки разделяются на опознавательные признаки и признаки деятельности. Опознавательные признаки описывают объекты в статическом состоянии: его назначение, принадлежность, параметры. Признаки деятельности объектов характеризуют этапы и режимы функционирования объектов, например, этап создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции, ее испытания и т. д. Все признаки объекта по характеру проявления можно разделить на 3 группы:

- внешнего вида - видовые демаскирующие признаки;
- признаки излучений - сигнальные демаскирующие признаки;
- материально-вещественные признаки.

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

Любое материальное тело с температурой выше абсолютного нуля (-273^0 С) излучает электромагнитные поля, обусловленные тепловым движением электронов атомов вещества. Кроме того, объект может содержать искусственно созданные источники полей или электрического тока. Наконец, в составе объекта могут находиться радиоактивные вещества. Радиоэлектронные средства излучают функциональные и побочные электромагнитные поля, механические движения частей приборов и машин создают акустические поля.

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

Вещественные признаки определяют физический и химический состав, структуру и

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

Важнейшим показателем признака является его информативность. Информативность можно оценивать мерой в интервале [0-1], соответствующей значению вероятности обнаружения объекта по конкретному признаку. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен.

Наиболее информативен именной признак, присущий только одному конкретному объекту. Такими признаками являются фамилия, имя, отчество человека, папиллярный узор его пальцев, инвентарный номер прибора или образца мебели. Не известны, например, факты о совпадении папиллярных узоров пальцев разных людей.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых прямыми, колеблется в пределах [0-1]. Признаки, непосредственно не принадлежащие объекту, но отражающие свойства и состояние объекта, называются косвенными. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Следы краски или характер деформации поверхности автомобиля в результате автодорожного происшествия позволяют находить автомобиль, скрывшийся с места происшествия. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако есть исключения, например, информативность четких отпечатков пальцев соответствует информативности именных признаков.

По времени проявления признаки могут быть:

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

Набор признаков, принадлежащих объекту, образуют его признаковую структуру Пст. Ее можно представить в виде объединения всех демаскирующих признаков объектов:

$$\text{Пст}\ (t) = \bigcup_{i=1}^{n} \prod_i^j (t),$$

где $\prod_i^j(t)$ - j-ое значение i-го признака в момент времени t.

В общем случае для описания объекта имеет значение не только количество и информативность признаков, но последовательность и время их проявления. Каждый i-ый признак обеспечивает возможность обнаружения объекта с вероятностью P_i. Если признаковая структура содержит n независимых признаков, то обнаружение объектов с помощью этих признаков повышается до величины $Q_n = 1 - \prod_{i=1}^{n} (1 - P_i)$.

Например, если вероятности обнаружения объекта по 5 признакам принимают значения: 0.017; 0.08; 0.021; 0.03; 0.015, то вероятность обнаружения его на основе этих признакам существенно выше и оценивается величиной более 0.15.

Если признаки зависимы, т. е. проявление какого-либо признака статистически связано с проявлением другого, то вероятность обнаружения объекта уменьшается по сравнению с вариантом независимых признаков. Например, значения признака “тень” при наблюдении объекта зависит от значения признака “размеры” и от взаимного пространственного положения объекта и внешнего источника света.

В общем случае признаковая структура представляет собой набор независимых или зависимых признаков, о которых достоверно известно, что они относятся к рассматриваемому объекту.

1.2.2. Видовые демаскирующие признаки

Видовые демаскирующие признаки описывают внешний вид объекта. Они объективно ему присущи, но выявляются в результате анализа внешнего вида модели (изображения) объекта на экране оптического приемника (сетчатки глаза человека, фотоснимке, экрана телевизионного приемника, прибора ночного видения и т. д.). Так как модель в общем случае отличается от оригинала, то состав и значения видовых демаскирующих признаков зависят не только от объекта, но и от условий наблюдения и характеристик оптического приемника. Наибольшее количество информативных видовых демаскирующих признаков добывается при визуально-оптическом наблюдении объектов в видимом диапазоне.

Основными видовыми демаскирующими признаками объектов в видимом свете являются:

- фотометрические и геометрические характеристики объектов (форма, размеры объекта, цвет, структура, рисунок и детали его поверхности);
- тени, дым, пыль, следы на грунте, снеге, воде;
- взаимное расположение элементов группового (сложного) объекта;
- расположение защищаемого объекта относительно других известных объектов.

Геометрические и фотометрические характеристики объектов образуют наиболее устойчивую и информативную информационную структуру, так как они присущи объекту и относятся к прямым признакам. Размеры объекта наблюдения определяются по максимальному и минимальному линейным размерам, площади и периметра проекции объекта и его тени на плоскость, перпендикулярную к линии визирования (наблюдения), высоте объекта и др.

Форма - один из основных демаскирующих признаков, прежде всего, искусственных объектов, поскольку для них, как правило, характерны геометрические правильные формы.

Размеры приобретают значение основного демаскирующего признака для объектов примерно одинаковой формы.

Детали объектов, их количество, характер расположения дают представление о сложном объекте и позволяют отличить его от подобных по форме.

Тени объектов возникают в условиях прямого солнечного освещения и являются важными демаскирующими признаками. По тени легче судить о форме и высоте объекта. Некоторые объекты (например, линии электропередач, антенные мачты, ограждения и т. д.) часто распознают только по тени. Различают два вида тени: собственную, которая ложится на поверхность самого объекта в зависимости от его формы, и падающую, отбрасываемую объектов на фон или поверхность других объектов. По падающей тени можно обнаружить объект, определить его боковые размеры, высоту, а также в ряде случаев и форму.

Важнейшим свойством поверхности объекта, определяющий его цвет и яркость, является коэффициент отражения поверхности на различных частотах: в видимом, инфракрасном и радиодиапазоне.

Объекты по-разному отражают падающие на них лучи света. Отражательные свойства объектов описываются коэффициентами (спектральным и интегральным) и индикатрисой отражения (рассеяния).

Графическое представление зависимости значений спектральных коэффициентов отражения от длины волны для различных объектов отличаются конфигурацией и положением максимума, что используется для различения объектов. Например, коэффициенты отражения растительности в инфракрасном диапазоне в несколько раз выше, чем в видимом, а коэффициенты отражения искусственных покрытий заметно не

отличаются. Например, коэффициент отражения от листвы летом в ближнем инфракрасном в 3-5 выше, чем в видимом, а от бетонных и асфальтовых покрытий изменяется незначительно. Индикатриса отражения характеризует распределение отраженного излучения в пространстве. Интегральный коэффициент отражения определяется в результате усреднения коэффициентов отражения для сравнительно широкого интервала длин волн.

В зависимости от фактуры поверхности различают направленное (зеркальное), рассеянное (диффузное) и смешанное отражение. Граница между ними условная и определяется соотношением величин неровностей поверхности и длины падающей волны. Поверхность считается зеркальной, если отношение среднеквадратичное значение высоты неровностей h к длине волны λ менее единицы, шероховатой, если более двух. Следовательно, шероховатая поверхность в видимом свете может в ИК-диапазоне выглядеть как зеркальная. Диффузное отражение присуще мелкоструктурным элементам, таким, как песок, свежевыпавший снег. Большинство объектов земной поверхности имеют смешанную индикатрису отражения, которая мало отличается от диффузной.

Яркость объекта, определяемая не только коэффициентами отражения объекта, но и яркостью внешнего источника освещения, относится к косвенным признакам, таким как дым, пыль, его следы на различных поверхностях.

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

При оценке излучений в инфракрасном диапазоне необходимо учитывать теплопроводность материалов объектов наблюдения. Нагреваясь от солнечных лучей, они к отраженному свету добавляют повышающуюся с ростом температуры долю собственных излучений. В диапазоне выше трех мкм мощность собственного теплового излучения объекта может превышать мощность отраженного им света.

В связи с этими свойствами в инфракрасном диапазоне появляется дополнительный признак - температура различных участков поверхности объекта по отношению к температуре фона.

Зрительный анализатор человека не воспринимает лучи в инфракрасном диапазоне. Поэтому видовые демаскирующие признаки в этом диапазоне добываются с помощью специальных приборов (ночного видения, тепловизоров), имеющих худшее разрешение, чем глаз человека. Кроме того, видимое изображение на экранах этих приборов одноцветное. Но изображение в инфракрасном диапазоне может быть получено при малой освещенности объекта или даже в полной темноте. В этом случае к демаскирующим признакам добавляются признаки, характеризующие температуру поверхности объекта.

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

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

В радиодиапазоне наблюдается более сложная картина, чем при отражении света. Отражательные возможности поверхности в этом диапазоне определяются, кроме указанных для света, ее электропроводностью и конфигурацией относительно направления падающей волны. Большая часть суши отражает электромагнитную волну в радиодиапазоне диффузно, спокойная водная поверхность - зеркально.

Радиолокационное изображение объектов сложной формы (автомобиль, самолет и др.) формируется совокупностью отдельных пятен различной яркости, соответствующих так называемым “блестящим точкам” объектов, отражающих сигнал в направлении радиолокационной станции (РЛС). “Блестящие точки” на экране локатора создают поверхности объектов, расположенных перпендикулярно направлению облучения, а также элементы конструкции, которые после переотражений внутри конструкции радиоволны к приемнику радиолокатора. Наибольшей отражающей способностью в направлении антенны радиолокационной станции обладают конструкции в виде 2-4-х жестко связанных между собой взаимно перпендикулярных металлических или металлизированных плоскостей. Такие конструкции называются уголковыми радиоотражателями, широко применяемыми для имитации ложных объектов.

Конкретный вид радиолокационного изображения зависит от положения объекта относительно направления облучения, так как при изменении ориентации меняется количество и взаимное положение “блестящих точек”.

Следовательно, размеры и форма радиолокационного изображения могут существенно меняться в зависимости от величины индикатрисы отражения и отличаться от подобных признаков, наблюдаемых в видимом свете. Отражательная способность объекта характеризуется эффективной площадью рассеяния.

Эффективная площадь рассеяния (отражения) соответствует площади плоской хорошо проводящей (металлической) поверхности, перпендикулярной к направлению облучения и помещенной в точке нахождения объекта и которая создает у приемной антенны радиолокационной станции такую же плотность потока мощности, как и реальный объект.

Эффективная площадь рассеяния человека составляет около 0.1-1 м^2, легкового автомобиля - около 3-5 м^2 , грузового автомобиля 7-10 м^2. В связи с сильной зависимостью значений эффективной площади рассеяния от пространственного положения объекта относительно направления на радиолокационную станцию имеет место большой разброс данных для одних и тех же объектов.

Кроме того, в зависимости от длины облучающая электромагнитная волна отражается не только от поверхности объекта, но и от более глубинных ее слоев. Проникающая способность в дециметровом диапазоне для сухой почвы, например, может составлять 1-2 м.

К основным видовым демаскирующим признакам объектов радиолокационного наблюдения относятся:

- геометрические и яркостные характеристики (форма, размеры, яркость, детали);
- эффективная площадь рассеяния;
- электропроводность поверхности;

Видовые демаскирующие признаки в радиодиапазоне добываются также с помощью тепловой радиолокации, приемники которой способны принимать сигналы собственных электромагнитных излучений и формировать на их основе изображения объектов. Так как возможности тепловых радиолокаторов весьма ограничены по разрешению и чувствительности, то демаскирующие признаки в радиодиапазоне позволяют выявлять меньший чем в видимом диапазоне набор признаков.

Таким образом, максимальное количество признаков внешнего вида объекта обеспечивают в видимом оптическом диапазоне фотоприемники с высоким разрешением, к которым в первую очередь относится глаз человека.

В инфракрасном диапазоне и в особенности в радиодиапазоне количество и качество признаков уменьшается. Отсутствует такой информативный признак как цвет. С увеличением длины волны ухудшается разрешение характеристик признака, например, точность оценки размеров объекта и его деталей. Если в инфракрасном диапазоне по изображению можно измерять объекты на местности с точностью до долей мм, то максимальное разрешение радиолокационных станций составляет единицы метров. Поэтому на радиолокационном изображении будут отсутствовать многие детали объекта, наблюдаемые на его изображении в оптическом диапазоне. Однако в инфракрасном и радиодиапазонах проявляются дополнительные признаки, которые в видимом диапазоне отсутствуют.

В радиодиапазоне яркость точки радиолокационного изображения зависит от электропроводности материала поверхности и эффективной площади рассеяния. Чем выше электропроводность поверхности объекта и больше площадь рассеяния, тем большая часть энергии отражается в направлении приемо-передающей антенны радиолокатора.

Следовательно, видовые демаскирующие признаки объектов и окружающей среды (фона) образуют признаковые структуры, отличающиеся в различных диапазонах длин электромагнитной волны. Эти свойства видовых демаскирующих признаков используются при комплексном добывании информации и их необходимо учитывать при организации защиты.

1.2.3. Сигнальные демаскирующие признаки

Понятие «сигнал» достаточно емкое и в общем случае обозначает условный знак для передачи на расстояние каких-нибудь сведений. В данных материалах под сигналом понимается носитель информации в виде поля или потока микрочастиц (электронов, ядер гелия).

Состав естественных и искусственных сигналов многообразен. К ним относятся собственные (обусловленные тепловым движением электронов, световые, радиоактивные) излучения объектов, отраженные от объектов поля и излучения, а также разнообразные созданные человеком источники электромагнитных излучений (радио и электрические устройства, приборы, средства). Последние могут рассматриваться как самостоятельные объекты защиты, например, радиостанции, так и входить в состав других объектов.

Классификация сигналов представлена на рис. 1.4.

Рис. 1.4. Классификация сигналов.

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

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

$s(t)=A\sin(\omega t+\varphi)$, где А-амплитуда, $\omega=2\pi f$-круговая частота колебания, φ - фаза

колебания.

Частота $f=\omega/2\pi$ измеряется в Гц и называется линейной.

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

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

где C_o - постоянная составляющая сигнала;

$C_к$ - амплитуда к-ой гармоники сигнала (к=1,2,.....,n);

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

Параметры ряда Фурье вычисляются по соответствующим формулам. Ряд Фурье представляет собой математическую модель периодического сигнала, также как любой цвет может быть разложен на составляющие красного, зеленого и синего цветов.

Совокупность гармонических составляющих сигнала образуют его спектр.

Амплитуда каждой спектральной составляющей характеризует энергию сигнала на соответствующей гармонике основной частоты. Чем выше скорость изменения амплитуды сигнала, тем больше доля в его спектре высокочастотных гармоник. Разность между максимальной и минимальной частотами спектра сигнала, между которыми сосредоточено основная часть, например, 95%, называется шириной спектра. Графическое изображение спектра периодического сигнала представлено на рис. 1.5.

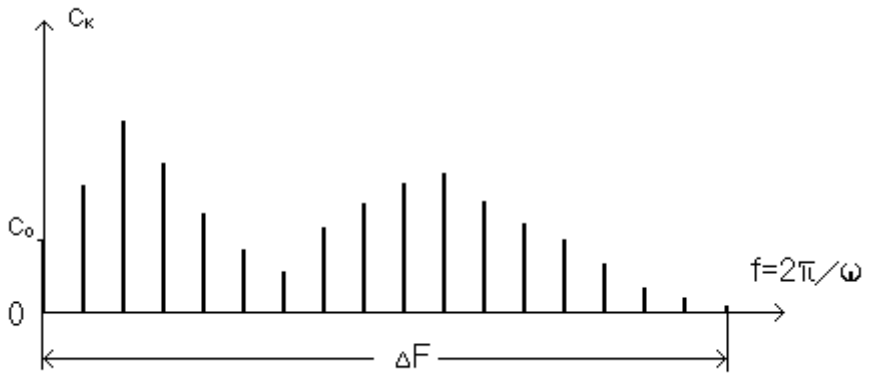


Рис. 1.5. Спектр периодического аналогового сигнала.

Частоты составляющих спектра непериодического аналогового сигнала непрерывно меняются. При наблюдении спектра такого сигнала на экране спектроанализатора положение и уровень различных спектральных составляющих непрерывно меняются и спектр выглядит как сплошной. В соответствии с изменением амплитуды аналогового сигнала меняется его энергия или мощность (так как мощность пропорциональна квадрату амплитуды). В зависимости от времени измерения энергии сигнала различают среднюю и мгновенную мощность. Десятичный логарифм отношения максимальной мощности сигнала к минимальной называется динамическим диапазоном сигнала.

Таким образом, аналоговый сигнал описывается набором параметров, являющихся его признаками. К ним относятся:

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

У дискретных сигналов амплитуда имеет конечный, заранее определенный набор значений. Наиболее широко применяется двоичный (бинарный) дискретный сигнал: в ЭВМ, в телеграфии, при передаче данных. Информационные сигналы, циркулирующие в

ЭВМ IBM PC, имеют значения амплитуды: 0 и 5 В. Осциллограмма бинарного сигнала показана на рис. 1.6.

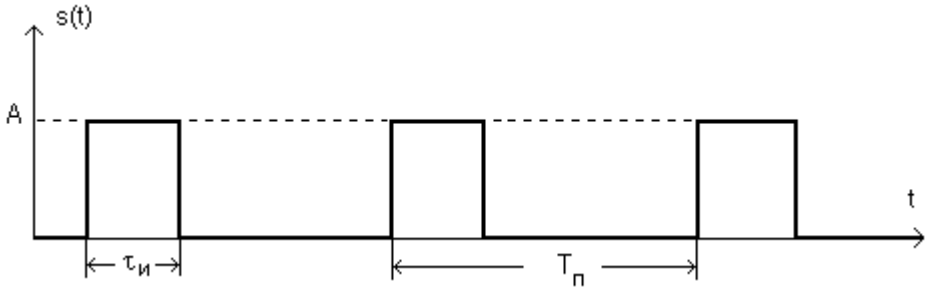


Рис. 1. 6. Осциллограмма бинарного сигнала.

Дискретный сигнал характеризуется следующими параметрами: амплитудой А и мощностью Р, длительностью импульса $\tau_и$ периодом $T_п$ или частотой $F_п = 1/T_п$ повторения импульсов (для периодических дискретных сигналов), шириной спектра сигнала ΔF_c, скважностью импульсов $\alpha = T_п/\tau_и$.

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

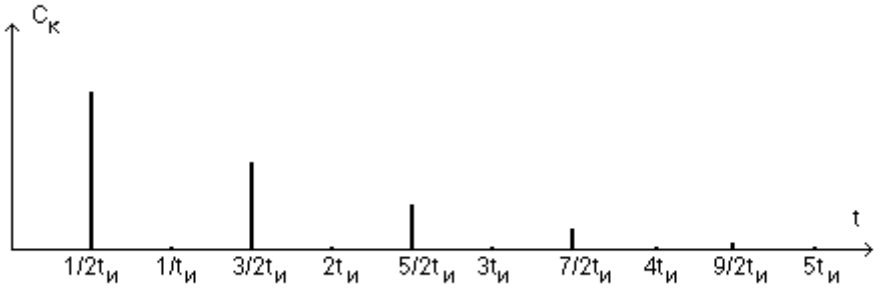


Рис. 1.7. Спектр бинарного сигнала.

Он характеризуется следующими свойствами:

- амплитуда гармонической составляющей $C_к$ уменьшается по закону $|\sin x/x|$;
- амплитуда гармоники $C_к$ обращается в ноль в точках $к/\tau_и$, к=1,2,...;
- в области частот спектра $(0 - 1/\tau_и)$ располагаются α -1 гармоник;
- постоянная составляющая сигнала равна A/α.

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

При прохождении дискретных сигналов по реальным электрическим цепям радиотехнических средств с ограниченной полосой пропускания их форма искажается и крутизна склона импульса уменьшается. Прямоугольный импульс приобретает колоколообразную форму. В результате этого размывается граница между амплитудой аналогового и дискретного сигналов. Искажения формы и уменьшение амплитуды импульсных сигналов в проводах ограничивают дальность их передачи, например, для обеспечения межмашинного обмена данными в локальных сетях.

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

Сигналы по виду передаваемой информации делятся на речевые, телеграфные, телекодовые, факсимильные, телевизионные, о радиоактивных излучениях и условные. Телеграфные и телекодовые сигналы используются для передачи буквенно-цифровой информации с низкой и высокой скоростью соответственно. Факсимильные и

телевизионные сигналы обеспечивают передачу неподвижных и подвижных изображений. Сигналы радиоактивных излучений являются демаскирующими признаками радиоактивных веществ. Условные сигналы несут информацию, содержание которой предварительно определено между ее источником и получателем, например, горшок с цветком на подоконнике - о провале явки в литературных произведениях о разведчиках.

Вид информации, содержащей в сигнале, изменяет его демаскирующие признаки: форму, ширину спектра, частотный и динамический диапазон. Например, стандартный речевой сигнал, передаваемый по телефонной линии, имеет ширину спектра 300-3400 Гц, звуковой - 16-20000 Гц, телевизионный - 6-8 МГц и т. д. Произведение $B=\Delta F_c \tau_c$ называется базой сигнала. Если $B\approx1$, то сигнал узкополосный. При $B>>1$ - сигнал широкополосный.

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

1.2.4. Вещественные демаскирующие признаки

Потребительские свойства изделий и товаров зависят не только и не столько от конструктивных и схемотехнических решений, но и от свойств материалов, из которых создаются эти товары и изделия. Поэтому состав, свойства и технология получения веществ с этими свойствами вызывают большой интерес у специалистов, а информация о них может быть чрезвычайно дорогой. Для обеспечения безопасности этой информации важно представлять признаки, по которым злоумышленник может воссоздать вещество с новыми свойствами. Классификация основных вещественных признаков представлена на рис. 1.8.

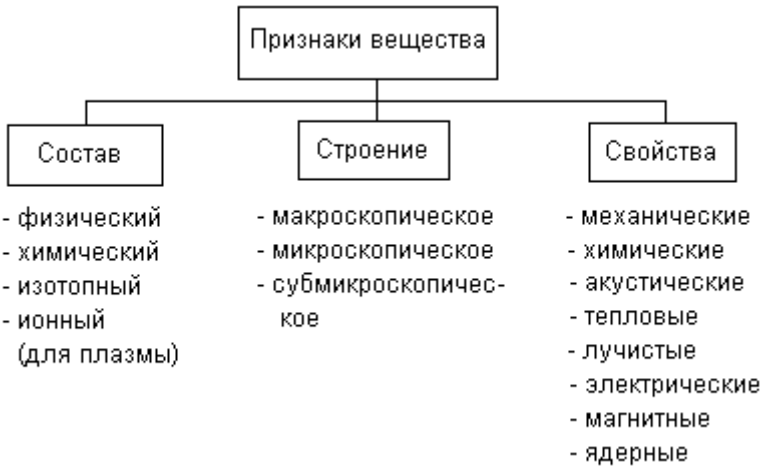


Рис.1.8. Классификация вещественных признаков.

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

По химическому составу вещества делятся на органические и неорганические. Химические элементы классифицируются в соответствии с периодической системой элементов Менделеева. Важнейшими классами неорганических соединений являются оксиды (вещества, состоящие из двух элементов, один из которых является кислород), кислоты, основания и соли.

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

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

Строение веществ различают на макроскопическом уровне, микроскопическом и субмикроскопическом (кристаллической решетки, макромолекул, молекул, субатомных частиц и атомов.

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

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

Акустические свойства определяют скорость передачи и поглощения звука в веществе.

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

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

Электропроводность, величины термо-эдс, окислительно-восстановительные потенциалы, потенциалы ионизации, диэлектрическая и магнитная проницаемость и т.п. характеризуют электрические и магнитные свойства вещества.

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

При решении задач защиты информации эти признаки рассматриваются как демаскирующие применительно к веществам и материалам, информация о которых относится к секретной (конфиденциальной). Вещества, содержащие демаскирующие вещественные признаки, называют демаскирующими веществами. В результате физико-химического анализа этих веществ добывается информации об их свойствах и технологии изготовления. Примером демаскирующих веществ служат радиоактивные вещества, демаскирующими признаками которых являются α, β, и γ-излучения. Альфа-излучение состоит из атомных ядер гелия с двойным положительным зарядом, движущихся со скоростью 14000-20000 км/с. Бета-излучение представляет собой электроны, скорости которых близки к скорости света. Гамма-излучение является электромагнитным излучением с длиной волны менее 100 мкм. Заряд и скорость (энергию) α и β-частиц определяют по их отклонению в электрическом и магнитном полях известной напряженности. Энергию и соответственно длину волны γ-излучения находят по энергии электронов, освобождаемых из различных веществ под действием этого излучения.

Потенциальные возможности выявления признаков демаскирующих веществ зависят от концентрации демаскирующих веществ при добывании. Минимально-допустимые значения концентрации демаскирующих веществ, исключающие получение злоумышленниками защищаемой информации, используются в качестве норм при обеспечении безопасности информации о вещественных признаках.

1.3. Источники и носители информации

1.3.1. Классификация источников и носителей информации

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

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, моделе 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. Даже при печатании на пишущей машинке остаются следы документов на копировальной бумаге и ленте, черновики или бракованные листы, которые неопытная или небдительная машинистка бросает в корзину для бумаг. Отходы производства в случае небрежного отношения с ними (сбрасывания на свалку без предварительной селекции, сжигания или резки бумаги и т. д.) могут привести к утечке ценной информации. Для такой возможности существуют 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.

1.3.2. 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 $F_{с,м}$, 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: $\Delta F_{ам}=2F_{с,м}$;
- для ЧМ: $\Delta F_{чм}>>F_{с,\ м}$;
- для ФМ: $\Delta F_{фм}\approx\Delta F_{чм}$.

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 D_c, шириной спектра частот ΔF_c и длительностью передачи T_c. Произведение этих трех параметров называется объемом сигнал $V_c=D_c\,\Delta F_c T_c$. В трехмерном пространстве объем сигнала можно представить в виде параллелепипеда (см. рис. 1.9).

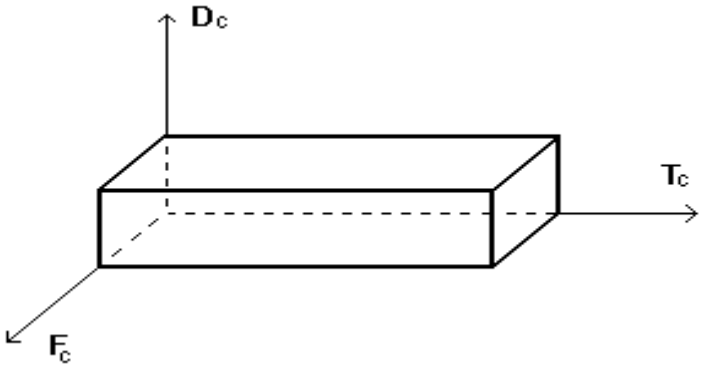


Рис. 1.9. Графическое представление объема сигнала.

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

1.4. Источники сигналов

Объекты, излучающие поля или потоки элементарных частиц, содержат источники сигналов. Если объект отражает поля внешних источников, то он одновременно является источником информации об объекте и источником сигнала. В этом случае сигнал содержит информацию о видовых или сигнальных признаках объекта. Например, сигнал в виде отраженного от объекта света несет информацию о свойствах его поверхности. В варианте, когда на вход источника сигнала поступает первичный сигнал, например, акустическая волна от говорящего человека, то источник сигнала, переписывающий информацию одного носителя (акустической волны) на другой (электромагнитное поле) в связи называется передатчиком. К таким источникам относятся, например, передающие устройства связных радиостанций. Источники сигналов, создаваемые и применяемые для обеспечения связи между санкционированными абонентами, называют функциональными источниками сигналов.

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

обеспечения целенаправленной защиты информации необходимо рассмотреть сущность источников сигналов.

1.4.1. Источники функциональных сигналов

К источникам функциональных сигналов относятся:
- передатчики радио и радиотехнические средств и систем;
- лазерные системы связи;
- излучатели акустических сигналов гидролокаторов и средств подводной связи;
- условные сигналы.

Средства радио и радиотехнических систем представляют наиболее многочисленную и разнообразную группу объектов, излучающих сигналы с семантической и признаковой информацией. К радиотехническим системам и средствам, передающим семантическую информацию, относятся:
- средства и системы радиосвязи;
- средства и системы телефонной связи;
- средства телеграфной и факсимильной связи;
- сети и аппаратура передачи данных;
- видео- и телевизионная аппаратура;
- электронно-вычислительная техника.
- радиолокационные и гидролокационные станции и системы;
- радионавигационные системы;
- радиотелеметрические системы;
- системы радиотелеуправления.

Средства и системы связи предназначены для обеспечения коммуникаций между людьми, а также техническими средствами. Они занимают ведущее место в обеспечении информационного обмена во всех сферах общественно-производственной деятельности и личной жизни людей.

Источники радиосигналов, излучаемых в окружающее пространство, являются радиопередающие устройства, а электрических сигналов, передаваемых по проводам, - телефонные, телеграфные, факсимильные аппараты, ЭВМ, образующие локальные сети на предприятии (организации) или выходящие во внешние сети вплоть до глобальных типа «Интернет». В последнее время для передачи информации в качестве источников сигналов применяются также лазеры. Уступая радиосигналам по дальности распространения, в особенности при неблагоприятных климатических условиях, лазерные системы имеют значительно лучшие параметры по полосе пропускания, помехоустойчивости и разрешению на местности.

Радио, электрические и световые сигналы с семантической информацией могут циркулировать как внутри организации, так и распространяться на большие, в принципе, на любые расстояния. По телефону можно переговорить с абонентом в любом месте Земли, радиосигналы способны донести информацию также до любой ее точки.
Учитывая широко применение средств связи и большие дальности распространения сигналов, добывание информации путем перехвата сигналов средств связи представляет один из эффективных и широко распространенных методов. Сигналы средств связи содержат информацию не только семантическую информацию, но и информацию о собственных признаках сигналов. Такая информация характеризует технические решения новых средств и их возможности, что представляет интерес как для внутреннего, так и для внешнего (зарубежного) конкурента.

Средства радиолокации и гидролокации, радионавигации, радиотелеметрии, радиотелеуправления, а также радиопротиводействия относятся к радиотехническим системам.

Среди радиотехнических систем и средств значительную долю занимают

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

Так как радио- и гидролокация являются основой для противоракетной, противовоздушной и противолодочной обороны, то признаки новейших локаторов вызывают большой интерес для разведки других государств. Очевидно, что сигнальные признаки разрабатываемых радио и акустических средств интересуют также фирмы - конкуренты в России и других государств, создающих подобную технику.

Радионавигационные средства и системы предназначены для определения местоположения объектов на суше, воде, в воздухе и в космосе. Радиотелеметрические средства и системы обеспечивают измерение и передачу различных физических величин удаленных объектов, а средства и системы радиотелеуправления - управления ими. К радиотехническим системам и средствам, характеристики сигналов которых интересуют органы добывания разведки, относятся также системы и средства радиопротиводействия (радиоэлектронной борьбы), предназначенные для нарушения системы управления войсками и оружием противника в военное время.

Передача коротких сообщений производится также условными сигналами. В качестве сигналов могут использоваться любые объекты наблюдения, излучения и материальные тела. Необходима только договоренность между источниками и получателями информации о содержании условного сигнала. Например, условными фразами часто пользуются люди во время конфиденциального разговора по открытому телефону.

1.4.2. Побочные электромагнитные излучения и наводки

Угрозу хищения информации путем ее утечки создают сигналы, случайно возникающие в результате побочных электромагнитных излучений и наводок (ПЭМИН). Эти сигналы называют также опасными.

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

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

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

- система внутриобъектового оповещения;
- система звукофикации залов заседаний и помещений для совещаний;
- средства телеграфной и факсимильной связи;
- система объектового промышленного телевидения;
- средства аудио- и видеозаписи, используемые для документирования защищаемой информации.

ВТСС включают:
- городскую и объектовую радиотрансляционную сеть вещания;
- систему электрочасофикации;
- технические средства охранной и пожарной сигнализации;
- телевизионные средства наблюдения системы охраны объекта;
- бытовые аудио- видеомагнитофоны;
- бытовые радиоприемники и телевизоры (без записи защищаемой информации);
- средства электропитания;
- бытовые электроприборы;
- электронные средства оргтехники.

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

Несмотря на многообразие типов средств источники опасных сигналов можно классифицировать исходя из их физической природе следующим образом:
- акустоэлектрические преобразователи;
- излучатели низкочастотных сигналов;
- излучатели высокочастотных сигналов;
- паразитные связи и наводки.

К акустоэлектрическим преобразователям относятся физические устройства, элементы, детали и материалы, способные под действием переменного давления акустической волны создавать эквивалентные электрические сигналы. Свойства акустоэлектрических преобразователей используются по своему функциональному назначению для создания микрофонов различных типов. Но существуют разнообразные радиоэлектронные и электрические элементы и устройства, обладающие так называемым «микрофонным эффектом», т. е. способными преобразовывать акустические сигналы в электрические. Это приводит к появлению в этих радио и электрических устройствах опасных сигналов, которые создают предпосылки для утечки информации. Классификация акустоэлектрических преобразователей, создающих опасные сигналы, приведена на рис. 1.10.

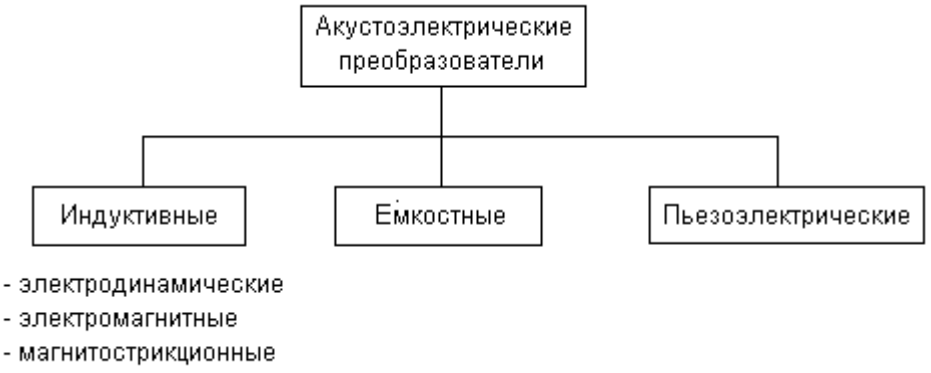


Рис. 1.10. Классификация акустоэлектрических преобразователей.

Электрические сигналы, модулированные акустическими сигналами, возникают в индуктивных акустоэлектрических преобразователях в результате перемещений под

действием акустических волн индуктивностей (катушек с металлической проволокой) в полях (магнитных и электрических) или при изменениях геометрических размеров катушек и их сердечников.

Наибольшей чувствительностью обладают электродинамические акустоэлектрические преобразователи в виде динамических головок громкоговорителей (см. рис. 1.11). Сущность преобразования состоит в следующем. Под давлением акустической волны катушка в виде картонного цилиндра с намотанной на нем тонкой проволокой перемещается в магнитном поле, создаваемом постоянным магнитом цилиндрической формы.

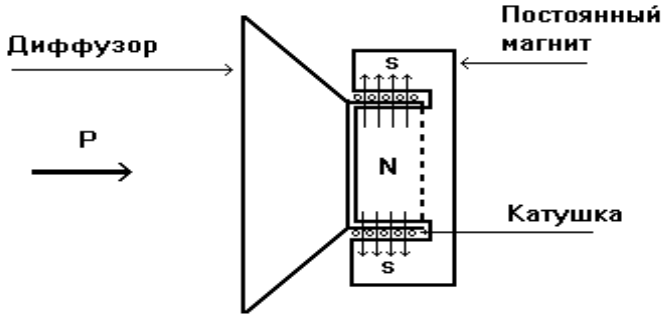


Рис. 1.11. Схема электродинамического громкоговорителя.

В соответствии с законом электромагнитной индукции в катушке (контуре) возникает электродвижущая сила (э.д.с.), величина которой пропорциональна громкости звука. Опасные сигналы на концах катушки составляют величину в 5 -15 мВ, достаточную для их распространения за пределы помещения, здания и даже территории. Поэтому не работающие, но непосредственно подключенные к радиотрансляционной сети громкоговорители или динамические головки устройств громкоговорящей связи, могут выполнять функцию микрофона и передавать информацию разговоров в помещении на достаточно большое расстояние.

Аналогичный эффект возникает в электромагнитных акустоэлектрических преобразователях. К ним относятся электромагниты электромеханических звонков и капсюлей телефонных аппаратов, шаговые двигатели вторичных часов, кнопочные извещатели ручного вызова пожарной службы охраняемого объекта и др. Электрические сигналы возникают в катушках электромагнитов этих устройств в результате изменений напряженности поля при изменениях под действием акустической волны воздушного зазора между сердечником и якорем электромагнита или статора (неподвижной части) и 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 из 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 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 индуктивности и модуляции циркулирующих в устройствах

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 схемы 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 на выходе акустоэлектрических преобразователей вызывают два вида угроз:

- распространение электрических опасных сигналов с информацией по проводам, выходящими за пределы контролируемой зоны, перехват которых злоумышленниками приведет к утечке информации;
- модуляция других, более мощных электрических сигналов или полей, к которым возможен доступ злоумышленников.

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

Иная ситуация с акустоэлектрическими преобразователями в телефонных аппаратах. Телефонные линии постоянно подключены к источнику электрического тока напряжением порядка 60 В. И хотя опасные сигналы на выходе звонковой сети составляют единицы и доли мВ, их нетрудно разделить с помощью фильтра от высоковольтного напряжения постоянного тока в телефонной линии. Постоянный ток фильтр не пропускает, а опасные сигналы с речевой информацией от акустоэлектрических преобразователей с частотами в диапазоне 300-3400 Гц проходят через фильтр с малым ослаблением, а затем усиливаются до необходимого значения.

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

виде электромагнитной волны. Также поля опасных сигналов на выходе акустоэлектрических преобразователей, которые сами по себе из-за малой напряженности не несут большой угрозы безопасности информации, могут наводить в цепях рядом расположенных радиоэлектронных средств электрические сигналы с аналогичным эффектом.

Опасные поля в виде низкочастотных полей образуются при протекании по токопроводам радиосредств (проводам индуктивностей, монтажным и соединительным проводам, дорожкам печатных плат) электрического тока в звуковом диапазоне частот с закрытой информацией. Источниками таких сигналов могут быть телефонные аппараты, устройства громкоговорящей связи, усилители мощности, бытовая радиоэлектронная аппаратура.

Характер поля зависит от расстояния до его источника и длины волны λ. В ближней зоне, в которой расстояние от источника r поля не превышает длину волны, преобладают электрическое или магнитное поля. Поле в ближней зоне называется полем индукции. Его энергия убывает пропорционально $1/ r^5$. В дальней зоне, начиная с расстояния, большего примерно 6λ от источника, электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами. В этой зоне происходит излучение части энергии и перенос ее во внешнее пространство на большие расстояния. Энергия убывает значительно медленнее (в $1/r^2$). С ростом частоты составляющая поля индукции уменьшается в соотношении 1/f, а составляющая поля излучения возрастает в зависимости f^2.

Поэтому энергия полей, частоты изменения которых относятся к звуковому диапазону, сосредоточена в ближней зоне. Однако если эти поля несут информацию, то она может быть в результате наведения 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.

Источниками побочных высокочастотных колебаний являются:

- высокочастотные генераторы, входящие в состав многих радиотехнических средств (телевизоров, радиоприемников, аудио- и видеомагнитофонов, 3-х программных абонентных громкоговорителей);
- усилительные каскады, в которых при определенных условиях возникают паразитные высокочастотные колебания;
- нелинейные элементы (диоды, транзисторы и другие активные радиоэлементы), на которые подаются гармонические высокочастотные колебания и электрические сигналы с речевой информацией.

Высокочастотные генераторы выполняют в радиотехнических приемниках функции генераторов гармонических колебаний, 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 модуляции колебаний.

Паразитные высокочастотные колебания в усилителях возникают при образовании между выходом и входом усилителя положительной обратной связи. 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. Промодулированные высокочастотные колебания распространяются в окружающее пространство и могут быть приняты за пределами территории организации.
Многочисленные опасные сигналы создают работающие ПЭВМ, в особенности в пластмассовых неметаллизированных корпусах. Ориентировочные дальности обнаружения радиоизлучений широко распространенных ПЭВМ зарубежного производства приведены в табл. 1.3.

Таблица 1.3.

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

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

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 наблюдается проникновение сигналов в непредназначенные 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 опасным в этом отношении цепям относятся, прежде всего, цепи питания и заземления. Цепи электропитания обеспечивают передачу электрической энергии от внешних источников (подстанций) подавляющему большинству устанавливаемых в помещениях радио и электрических приборов в виде переменного электрического тока напряжением 220 В и частотой 50 Гц. В любом радиотехническом изделии имеется собственный блок (узел) питания, который преобразует напряжение 220 В переменного тока в требуемые для нормальной работы прибора значения напряжения постоянного и переменного тока. Например, для питания всех устройств ПЭВМ его блок питания формирует напряжения +5, -5, -12, +12 В постоянного тока. 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. Различие в частотах питающего напряжения 50 Гц и сигнала в диапазоне частот речи позволяет в принципе выделить с помощью частотных фильтров опасный сигнал чрезвычайно малой амплитуды на фоне напряжения 220 В. Хотя блок питания сглаживает колебания тока в сети электропитания, вызванные циркулирующими в технических средствах информационными сигналами, но существует реальная возможность утечки информации через цепи питания от звукоусиливающей аппаратуры.

Цепи заземления предназначены для обеспечения защиты электрических сигналов с информацией от помех и наводок путем экранирования проводов или устройств. При воздействии на экраны побочных электрических и электромагнитных полей на последних 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 земли на глубину 1-2 м для обеспечения хорошего контакта с токопроводящими слоями. Протекающие по цепи заземления опасные сигналы могут перехвачены приемной аппаратурой злоумышленника.

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

Паразитная индуктивная связь проявляется в ходе следующих физических процессов. В пространстве, окружающем любую цепь, по которой протекает электрический ток I, возникает магнитное поле, постоянное или переменное с частотой (в соответствии с характером тока. В соседних проводниках, находящихся в переменном магнитном поле, возбуждаются переменные э.д.с. $E=I\omega M$, где M - взаимная индуктивность. Величина M пропорционально индуктивности влияющих друг на друга элементов цепей и обратно пропорциональна расстояния между ними. Например, взаимоиндуктивность двух медных прямых параллельных проводников длиной 100 мм и толщиной 0.02 мм при интервале между ними 2 мм составляет 0.07 мкГн, а при интервале 10 мм - 0.04 мкГн.

Емкостная паразитная связь возникает между любыми элементами схемы, прежде всего, между параллельно расположенными проводами, а также точками схемы и корпусом (шасси). Емкостная связь зависит от геометрических размеров элементов цепей и расстояния между ними. Например, емкость между двумя параллельными проводами длиной 100 мм и диаметром 0.1 мм уменьшается с 0.75 пф до 0.04 пф при увеличении расстояния между ними с 2 до 50 мм. Для проводов диаметром 2 мм эта емкость при тех же условиях снижается с 5 пф до 0.07 пф.

Из-за паразитных индуктивных и емкостных связей возникают паразитные наводки. Под паразитной наводкой понимается передача напряжения из одного элемента радиоустройства в другой, не предусмотренная его схемой и конструкцией. Принципы паразитной наводки иллюстрируются рис. 1.12.

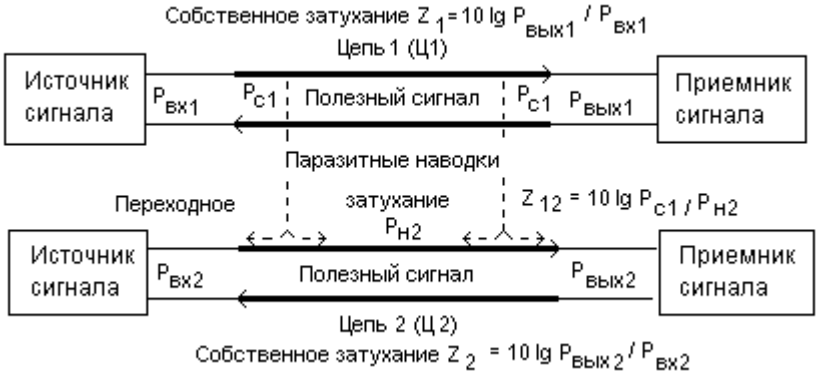


Рис. 1.12. Принципы паразитной наводки

Когда ток проходит по проводам (жилам) первой цепи (Ц1), вокруг них создается электрическое поле, силовые линии которого пронизывают провода (жилы) второй цепи (Ц2). Аналогичная схема магнитного влияния между цепями. В результате этого по цепи Ц2 потечет помимо основного еще и переходной ток, создающий помеху основному. Защищенность от взаимных помех оценивается так называемым переходным затуханием $Z_{12} = 10\lg P_{с1}/P_{н2}$, где P_1 и $P_{н2}$ - мощность сигналов в 1-й цепи и наводки от них во 2-й цепи. Переходное затухание для надежной защиты информации должно быть не менее величины $10\lg P_с/P_{пр}$, где $P_с$ и $P_{пр}$ - мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал.

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

Глава 2. Характеристика угроз безопасности информации

2.1. Виды угроз безопасности информации

Под безопасностью информации понимаются условия, при которых она не подвергается опасности. Опасность (по Ожегову С. И.) - угрозы чего-либо. Следовательно, под безопасностью информации следует понимать условия хранения, обработки и передачи информации, при которых обеспечивается ее защита от угроз уничтожения, изменения и хищения.

Следует различать потенциальную и реальную безопасность. Потенциальная безопасность информации, как и любого другого объекта или субъекта, существует всегда. Безопасность информации оценивается двумя показателями: вероятностью предотвращения угроз и временем, в течение которого обеспечивается определенный уровень безопасности. Эти показатели взаимозависимые. При заданных конкретных мерах по защите обеспечить более высокий уровень безопасности возможно в течение более короткого времени.

Так как информация содержится в значениях параметров носителя, то эти параметры должны сохранять свои значения в течение определенных значений. Очевидно, что параметры носителя постоянно меняются. Бумага со временем изменяет свой цвет, становится ломкой и хрупкой. Но если текст, напечатанный на ней, читается без искажений, то можно говорить об обеспечении безопасности содержания информации. Однако когда текст, например, содержит цветные изображения (рисунки или цветные репродукции), то ухудшение яркости или изменение красок меняют количество информации в изображении. В этом случае информация искажается. Для замедления процесса изменения параметров бумаги в хранилищах книг и картин принимают специальные меры по обеспечению безопасности информации путем уменьшения влияния угроз со стороны факторов среды хранения: поддерживают определенную температуру и влажность воздуха.

С угрозами безопасности информации постоянно сталкиваются пользователи вычислительной техники. Информация, записанная на магнитных дисках, со временем теряется или искажается в результате осыпания магнитного порошка или размагничивания отдельных участков магнитного слоя дисков, дискет и лент.

Информация постоянно подвергается случайным или преднамеренным воздействиям - угрозам: хищению, изменению, уничтожению. В общем случае эти угрозы реализуются в результате:

- действий злоумышленников: людей, занимающихся добыванием информации в интересах государственной и коммерческой разведки, криминальных элементов, непорядочных сотрудников или просто психически больных людей;
- разглашения информации людьми, владеющими секретной или конфиденциальной информацией;
- утери носителей с информацией (документов, машинных носителей, образцов материалов и др.);
- несанкционированного распространения информации через поля и электрические сигналы, случайно возникающие в электрических и радиоэлектронных приборов в результате их старения, некачественного конструирования (изготовления) и нарушений правил эксплуатации;
- воздействий стихийных сил, прежде всего, огня во время пожара и воды в ходе тушения пожара и протечками в трубах водоснабжения;
- сбоев в работе аппаратуры сбора, обработки, хранения и передачи информации, вызванных ее неисправностями, а также непреднамеренных ошибок пользователей или обслуживающего персонала;
- воздействия мощных электромагнитных и электрических промышленных и природных помех.

Несанкционированное распространение (утечка) информации может происходить в результате:

- наблюдения за источниками информации;
- подслушивания конфиденциальных разговоров и акустических сигналов;
- перехвата электрических, магнитных и электромагнитных полей, электрических сигналов и радиационных излучений;
- несанкционированного распространения материально-вещественных носителей за пределы организации.

Наблюдение включает различные формы: визуальное, визуально-оптическое (с помощью оптических приборов), телевизионное и радиолокационное наблюдение, фотографирование объектов в оптическом и инфракрасном диапазонах.

Учитывая распространенность акустической информации при общении людей, подслушивание, прежде всего, речевой информации вызывает одну из наиболее часто встречающихся угроз безопасности информации - ее копирование. Подслушивание звуков, издаваемых механизмами во время испытаний или эксплуатации, позволяет специалистам определить конструкцию, новые узлы и технические решения излучающих эти звуки механизмов. Перехват полей и электрических сигналов, содержащих информацию, осуществляется путем их приема злоумышленником и съема с них информации, а также анализа сигналов с целью получения сигнальных признаков.

Угрозу безопасности информации создают также условия и действия, обеспечивающие попадание к злоумышленнику бумажных носителей (набросков, черновиков и др.), бракованной продукции или ее отдельных узлов и деталей, сырья и материалов, содержащих демаскирующие вещества, и других источников информации.

Наблюдение, перехват и подслушивание информации, проводимые с использованием технических устройств, приводят к ее утечке по техническим каналам.

Для обеспечения эффективной защиты необходимо оценивать величину угрозы. Величину конкретной угрозы C_{yi} для рассматриваемого i-го элемента информации в общем случае можно представить в виде произведения потенциального ущерба от реализации угрозы по i-му элементу информации $C_{пyi}$ и вероятности реализации угрозы P_{yi}, т. е. $C_{yi}=C_{пyi}\,P_{yi}$.

Получить точные количественные значения сомножителей не представляется

возможным. Приближенная оценка угрозы возможна при следующих ограничениях и условиях.

Во-первых, можно предположить, что максимальный ущерб от хищения информации соответствует ее цене. Действительно, в случае попадания информации к конкуренту владелец информации может лишиться не только ожидаемой прибыли, но и не компенсировать ее себестоимость.

Во-вторых, в условиях полной неопределенности знаний о намерениях злоумышленника по добыванию информации ошибка прогноза минимальна, если принять величину вероятности реализации угрозы в течение рассматриваемого периода времени (например, 1 года) равной 0.5.

В результате усреднения по всем i - м элементам информации верхняя граница угрозы составит половину цены защищаемой информации. Очевидно, что чем выше цена информации и больше угроза ее безопасности, тем больше ресурсов потребуется для защиты этой информации.

2.2. Органы добывания информации

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

Любое государство создает органы разведки, обеспечивающие руководство страны информацией для принятия им политических, экономических, военных, научно-технических решений в условиях жесткой межгосударственной конкуренции. В зависимости от целей государства, его внешней политики и возможностей структуры органов разведки существенно отличаются.

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

1. Центральное разведывательное управление (ЦРУ).
2. Разведывательные организации Министерства обороны США.
3. Разведывательные организации, входящие в гражданские ведомства США.
4. Штаб разведки разведывательного сообщества или Центральная разведка.

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

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

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

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

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

Директорат планирования занимается планированием и координацией деятельности разведки.

В число разведывательных подразделений Министерства обороны входят:

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

Основными подразделениями разведки Министерства обороны являются:

- разведывательное управление Министерства обороны (РУМО), занимающегося военно-стратегической разведкой;
- Агентство национальной безопасности (АНБ), осуществляющего в контакте с ЦРУ сбор информации с помощью радиоэлектронной разведки, а также разработку кодов и шифров. Оно располагает одним из самых крупных центров по обработке данных самыми мощными ЭВМ, обслуживает около 2 тыс. станций радиоэлектронного перехвата, численность персонала составляет более 120 тыс. человек.

К разведывательным организациям гражданских ведомств США относятся:

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

Разведка Госдепартамента США обеспечивает сбор информации, необходимой для проведения внешней политики США, участвует в разработке разведывательных операций и национальной разведывательной программы США.

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

Кроме того, секретная служба Министерства финансов обеспечивает охрану президента и вице-президента, членов их семей, официальных гостей правительства, охрану правительственных зданий. Она насчитывает 1.5 тыс. сотрудников, занимается сбором информации об организациях и лицах в США и за рубежом, которые могут представлять потенциальную опасность для охраняемых лиц и объектов.

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

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

В целях снижения дублирования деятельности многочисленных организаций, собирающих разведывательную информацию в интересах различных ведомств страны, координацию деятельности всех организаций разведывательного сообщества осуществляет штаб центральной разведки, который возглавляет директор ЦРУ.

Разведывательным сообществом развернута разведывательная сеть практически во всех странах мира, разведкой занимаются сотни тысяч штатных сотрудников и привлекаемых специалистов. Возможности разведывательного сообщества достигает уровней бюджета развивающихся стран. В начале 90-х годов общие расходы на американскую разведку составляли по данным печати около 60 млрд. долл. ежегодно.

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

Основными сферами интересов разведки государства являются:

- состояние военно-экономического и научно-технического потенциалов других государств, прежде всего, потенциальных противников, и прогнозирование их развития;

- размещение военно-технических объектов, их производственные мощности, характер и распределение выпускаемой продукции;
- содержание и характер работ, ведущих в области создания новых видов вооружения и военной техники;
- состав и дислокация группировок войск и сил флота;
- эффективность вооружения и военной техники, их тактико-технических характеристик;
- масштаб проводимых учений, состав привлекаемых на них сил и средств, содержание решаемых на учениях задач;
- принципы построения и технического оснащения систем государственного и военного управления;
- инженерное оборудование континентальных и навигационно-гидрографического обеспечения океанских театров военных действий;
- наличие топливо-энергетических, рудных, водных, растительных и других природных ресурсов;
- метеорологические условия на территории разведуемых государств;
- выполнение условий международных договоров, прежде всего, об ограничении вооружений.

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

Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности на рынке в условиях острой конкурентной борьбы.

Задачи органов коммерческой разведки, их состав и возможности зависят от назначения и капитала фирмы, но принципы добывания информации существенно не отличаются. Основными областями, представляющие интерес для коммерческой разведки, являются следующие:

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

Задачи разведки коммерческих структур включают:

- изучение и выявление организаций, потенциально являющихся союзниками или конкурентами;
- добывание, сбор и обработка сведений о деятельности потенциальных и реальных конкурентов;
- учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами;

- оценка реальных отношений между сотрудничающими и конкурирующими организациями;

- анализ возможных каналов утечки конфиденциальной информации.

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

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

Органы коммерческой разведки входят в состав в службы безопасности (СБ) организации, вариант структуры которого приведен на рис. 2.1.

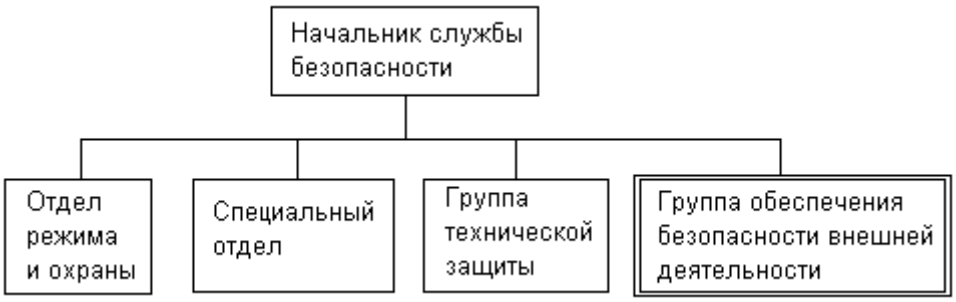


Рис. 2.1. Вариант структура службы безопасности предприятия.

В общем случае органы разведки образуют систему разведки с многоуровневой иерархической структурой (рис. 2.2).

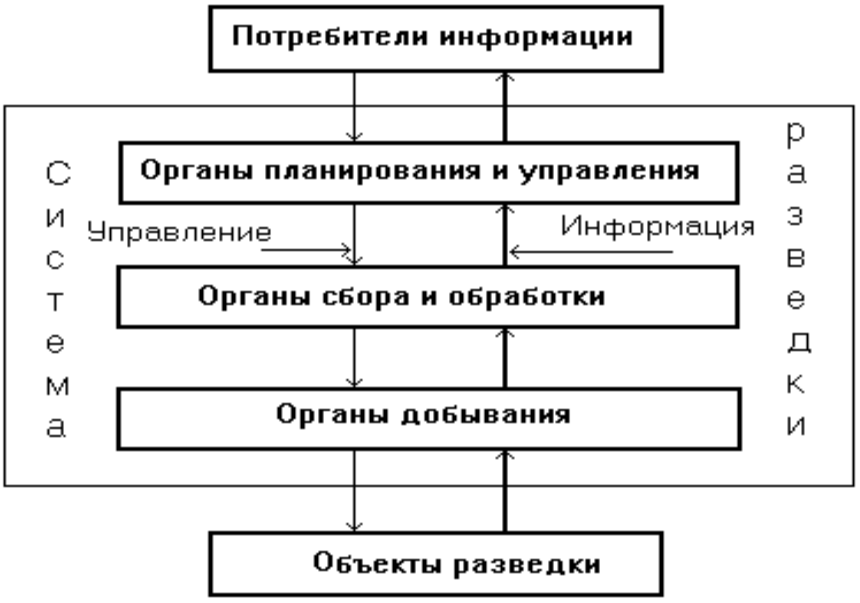


Рис. 2.2. Структура системы разведки.

Такой схеме необязательно соответствует административная структура органов

государственной или коммерческой разведки. Необходимость указанных уровней обусловлена объективными процессами добывания информации. В минимальном варианте функции системы добывания информации могут быть реализованы одним или несколькими работникам службы безопасности малочисленной фирмы.

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

В соответствии с поставленными задачами и планом проведения операции органы добывания обеспечивают разведывательный контакт с источниками информации и получают от них данные и сведения. Редко органам добывания удается получить их в объеме и с качеством, достаточными для ответа на поставленные вопросы. Как правило, добываемые данные и сведения разрозненные и малоинформативные. Поэтому сбор и обработка добытых сведений и данных, а также доведение информации до потребителя производится органами сбора и обработки разведки.

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

В настоящее время достаточно условно разведку можно разделить на агентурную и техническую. Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия - в преобладании человеческого или технического факторов.

Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента - разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

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

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

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

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

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

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

Оптическая разведка включает:

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

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

Радиоэлектронная разведка в зависимости от характера добываемой информации подразделяется на:

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

Радиоразведка добывает семантическую информацию путем перехвата радиоизлучений с конфиденциальной информацией, радиотехническая - информацию о параметрах (признаках) радиотехнических сигналов, радиолокационная - о видовых признаках радиолокационного изображения объекта на экране радиолокатора, наконец, радиотепловая - о признаках объектов, проявляющихся через их собственные электромагнитные излучения в радиодиапазоне.

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

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

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

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

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

Рассмотренное многообразие видов разведки обеспечивает добывание информации, представленной на всех известных в природе носителях.

2.3. Принципы ведения разведки

Основными принципами ведения разведки являются следующие:

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

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

основных задач.

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

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

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

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

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

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

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

2.4. Технология добывания информации

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

Легальное добывание информации проводится путем изучения и обработки публикаций по интересующих разведку вопросом в средствах массовой информации, периодических научных и популярных журналах, трудах ВУЗОВ и научно-производственных акционерных обществ, правительственных изданиях, учебных пособиях и др. Ценную информацию можно получить из правительственных источников, отчетов компаний по операциям с ценными бумагами, в местных юридических ведомостях, из судебных материалов, освещающих ход судебного разбирательства с участием конкурента, и из других источников.

Нужную информацию можно найти в материалах, имеющих непосредственное отношение к деятельности фирмы: в соглашении о лицензиях, статьях и докладах, годовых отчетах фирм, отчетах коммивояжеров, обзорах рынков и докладов инженеров-консультантов, внутренних печатных изданиях, телефонных справочниках, рекламной литературе и проспектах. Этот перечень можно многократно продолжить.

Органы обработки информации зарубежной разведки выписывают практически всю открытую центральную и местную печатную продукцию. По статистике около объема

90% информации разведка получает из открытых источников.

Однако наиболее ценная информация добывается нелегальным путем, в результате проведения тайных мероприятий спецслужбами и органами коммерческой разведки или так называемого промышленного шпионажа. Последний термин представляет журналистский жаргон и вместо него целесообразно применять термин «коммерческая разведка».

Добывание информации в общем случае представляет процесс, который начинается с момента постановки задачи ее пользователями (военно-политическим руководством страны или отдельных ведомств, руководством фирмы) до момента предоставления пользователям информации, соответствующей поставленным задачам и требованиям. Технология добывания информации включает следующие этапы:

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

Организация добывания информации предусматривает:

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

Поставленные в достаточно общем виде задачи на добывание необходимой пользователям информации нуждаются в конкретизации с учетом имеющейся априорных данных о возможных источниках информации, их нахождении, возможных способах доступа и преградах, возможностях имеющихся технических средств добывания и т. д. В результате анализа задач и априорных данных разрабатывается замысел операции, в котором намечаются пути решения поставленных задач.

На результативность добывания информации влияют многочисленные мешающие и случайные факторы - противодействие контрразведки и службы безопасности, недостаточность априорной информации об источниках добываемых сведений и данных, отказы аппаратуры, погодные условия, бдительность граждан и сотрудников организации и др. Эти факторы учитываются при планировании действий с указанием места и времени действий всех субъектов и технических средств, участвующих в операции по добыванию информации. Нормативное управление предусматривает постановку задач исполнителям перед проведением разведывательной операции, оперативное - внесение в ходе добывания информации корректив в план, вызванных изменениями обстановки. Организацией добывания информации занимаются органы планирования и управления.

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

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

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

Эталонные признаковые структуры содержат достоверные (по оценке органа

добывания) признаки объекта или сигнала, полученные от первоисточников, например, из документа или по данным, добытым из разных источников. Например, фотография в паспорте является эталонным описанием лица конкретного человека. Его признаковая структура состоит из набора признаков лица, которые криминалисты используют для составления фотороботов. Эталоны по мере изменения признаков корректируются. Например, несколько раз в течение жизни человека заменяются фотографии в паспорте, которые представляют собой эталонные изображения владельца паспорта для идентификации его личности. Эталонные признаковые структуры об объектах окружающего мира человек хранит в своей памяти. Он постоянно их формирует в процессе развития, обучения и работы. Когда человек рождается, у него отсутствуют эталонные признаковые структуры объектов окружающего мира. В процессе собственных наблюдений и опыта, полученных знаний у него постепенно и постоянно формируются эталонные признаковые структуры, которые со временем корректируются. Например, когда человек встречает через 20 лет одноклассника, внешний вид которого существенно изменился, то вначале он может и не узнать своего бывшего приятеля, так как наблюдаемые (текущие) признаки отличаются от эталонных двадцатилетней давности. После получения семантической информации о том, что текущие признаки действительно принадлежат его школьному приятелю, в памяти производится корректировка эталона и при следующей встрече сомнения не возникают.

Путем идентификации текущей признаковой структуры с эталонной человеком или автоматом производится обнаружение объекта, которому соответствует эталонная признаковая структура. Чем больше признаков совпадает, тем выше вероятность обнаружения объекта.

Если эталонная признаковая структура отсутствует или принадлежность их объекту вызывает сомнение, то процессу поиска объекта разведки предшествует этап поиска его эталонных (достоверных) признаков. Эталонные признаковые структуры постоянно накапливаются и корректируются при получении достоверных признаков. Полнота и достоверность эталонных признаковых структур для всех объектов, интересующих разведку или любую другую структуру, например, провоохранительные органы, определяют необходимое условие эффективного обнаружения объекта.

Добытые данные, как правило, разрозненные. Они преобразуются в информацию, отвечающую на поставленные задачи, в ходе информационной работы, выполняемую органами сбора и обработки информации.

Информационная или аналитическая работа включает следующие процессы:

- сбор данных и сведений от органов добывания;
- видовая обработка;
- комплексная обработка.

Взаимосвязь этих процессов представлена на рис. 2. 3.

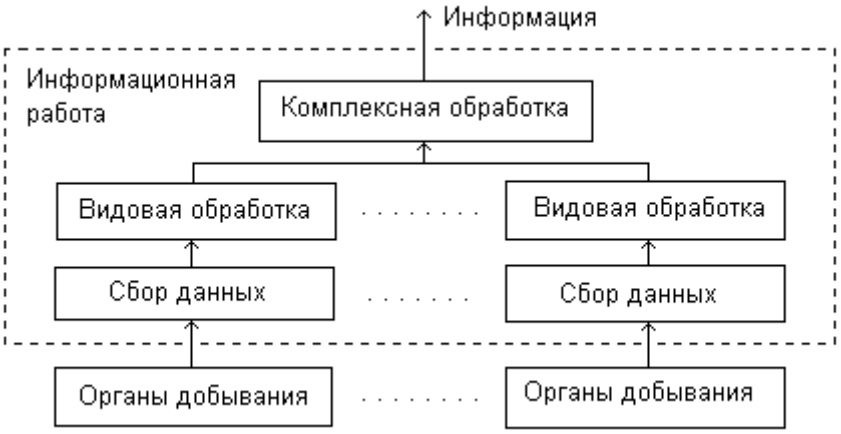


Рис. 2.3. Структура процессов информационной работы

Данные и сведения (в случае предварительной обработки данных в органе

добывания) передаются в орган видовой обработки. Если в добывании информации участвуют органы различных видов, например, оптической и радиоэлектронной разведки, то осуществляется комплексная обработка сведений, поступивших от органов видовой обработки. Необходимость видовой обработки обусловлена различиями языков признаков, добываемых органами различных видов.

В ходе видовой и комплексной обработки формируются первичные и вторичные сведения на основе методов синтеза информации и процедур идентификации и интерпретации данных и сведений.

Формирование первичных сведений производится путем сбора и накопления данных и "привязки" их к тематическому вопросу, по которому добывается информация. Для включения данных в первичные сведения необходимо, чтобы эти данные содержали информационный признак о принадлежности данных к информации по конкретному вопросу. Например, если поставлена задача добывания информации о новом автомобиле, то добытые признаки его внешнего вида могут быть отнесены к этому автомобилю, если существует дополнительный признак (место, время или наличие возле него определенных лиц), которые с высокой степенью достоверностью указывают о принадлежности признаков этому автомобилю. Если такой признак отсутствует, то имеет место простое накопление данных.

Формально при наличии в добытых данных Ах, Вх и Сх общего признака х, характеризующего принадлежность их к одному и тому же тематическому вопросу или объекту, если речь идет об объекте разведки, данные объединяются в первичные сведения АВСх. Любые новые данные, полученные от органа добывания, «привязывают», если это возможно, по общему признаку к первичным сведениям соответствующего объекта. В результате этого по мере добывания новых данных об объекте разведки его признаковая структура пополняется новыми признаками, что приводит к увеличению различия ее по отношению к признаковым структурам других объектов.

Если полученные сведения отвечают на поставленные перед разведкой вопросы, то содержащая в сведениях информация, семантическая и признаковая, в соответствующей форме передается ее потребителям.

Необходимость в формировании вторичных сведений возникает тогда, когда не совпадают языки итоговой информации и первичных сведений, получаемых от органов добывания. Если потребителя информации интересует видовые свойства продукции, создаваемой конкурентом, то добытые признаки внешнего вида не нуждаются в дополнительной обработке. Но когда для потребителя важны методы работы разрабатываемого технического средства, то первичные признаки не отвечают на эти вопросы. В этом случае формируются вторичные сведения не в виде, например, признаков внешнего вида или признаков сигналов, а в виде описания конструкции узлов и деталей новой продукции, которые не удается добыть в виде оригиналов или копий.

Однако специалисты по внешнему виду могут в принципе по видовым признакам выявить особенности конструкции и работы продукции. Эти особенности не содержатся в первичных сведениях, у них даже разные языки. При формировании вторичных сведений возникает новая информация. Генерация новой информации возникает в результате интерпретации (толковании) первичных сведений. Интерпретация - это высшая форма обработки информации, присущая в настоящее время только человеку.

В случае когда вторичные сведения не отвечают на поставленные перед разведкой вопросы, из них по аналогии с первичными формируют вторичные сведения

При формировании сведений применяются следующие методы синтеза информации:

- логические;
- структурные;
- статистические.

Логические методы используют для синтеза информации законы логики,

учитывающие причинно-следственные связи в реальном мире. Они лежат в основе так называемого «здравого смысла» человека и являются основным методом синтеза информации человеком. Здравый смысл по существу представляет интегральную оценку результатов обработки информации человеком на бессознательном уровне. Чем большими знаниями и опытом владеет человек, тем больше информативных связей он учитывает при принятии решения. Однако эти связи имеют и обратную сторону. Они консервируют логику мышления человека и тормозят процесс генерирования им новой информации ограничениями типа «этого не может быть». Люди, обладающие бурной фантазией, но лишенные консерватизма специальных знаний и опыта, - писатели-фантасты создают в своих произведениях модели будущих образцов научно-технического прогресса, на десятилетия опережающие время их создания. В то же прогнозы специалистов часто похожи на прототипы.

Причинно-следственные временные связи обеспечивают также выявление и прогнозирование действий объектов по признакам их деятельности в различные моменты времени.

Структурные методы учитывают объективно существующие связи между элементами объекта. Например, в общем случае продукция, выпускаемая фирмой, имеет многоуровневую иерархическую структуру. Она содержит блоки, узлы и детали, которые взаимодействуют друг с другом. Эти связи определяют конструкцию прибора или любого другого товара и зафиксированы в конструкторской документации. При ее отсутствии специалисты восстанавливать конструкцию, назначение и функции по отдельным элементам и связям.

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

Таким образом, информационная работа включает обработку больших массивов данных и сведений. Органы разведки широко привлекают к информационной работе в качестве аналитиков высококвалифицированных специалистов, которые увязывают разрозненные и противоречивые данные и сведения (в первичные и вторичные) и производят их интерпретацию на языке пользователя информации. Кроме того, проводятся интенсивные работы по автоматизации процессов информационной работы.

2.5. Способы доступа к конфиденциальной информации

Возможности разведки по добыванию информации зависят, прежде всего, от способов доступа ее органов добывания (агентов, технических средств) к источникам информации и обеспечения разведывательного контакта с ними. Эти факторы связаны между собой. Чем ближе удается приблизиться органу разведки к источнику информации, тем выше вероятность установления разведывательного контакта с ним. Доступ к информации предполагает, что источник (или носитель информации) обнаружен и локализован и с ним потенциально возможен разведывательный контакт. Разведывательный контакт между злоумышленником или его техническим средством и источником информации предусматривает установление физического контакта между злоумышленником (техническим средством) и носителем информации. Физический контакт предполагает, что злоумышленник имеет возможность взять носитель с информацией в руки с целью его хищения, копирования, уничтожения или модернизации или с помощью своих рецепторов и используемых технических средств добывания - снять

с носителя информацию дистанционно.

В общем случае под разведывательным контактом понимаются состояние источника информации или сигнала, среды распространения и несанкционированного получателя, для которых выполняются пространственное, энергетическое и временное условия.

Пространственное условие предполагает такую взаимную пространственную ориентацию источника информации и злоумышленника, при котором злоумышленник «видит» источник информации с помощью своих органов чувств или технических средств добывания.

Так как любое перемещение носителя в пространстве приводит к уменьшению его энергии, то энергетическое условие разведывательного контакта определяет необходимость обеспечения энергии носителя на входе приемника злоумышленника, достаточного для получения на его выходе информации с требуемым качеством. Энергетическое условие учитывает не только энергию или мощность носителя, но и уровни различного рода мешающих воздействий (помех) одинаковой с носителем информации физической природы. Помехи присутствуют в любой среде распространения и создаются в любом приемнике. Они могут при недостаточной мощности носителя (сигнала) вызвать такие искажения информации, при которых она станет непонятной получателю или у него возникнут сомнения в достоверности, особенно цифровых данных, которые наиболее легко подвергаются трансформации под действием помех. Поэтому получатель информации (санкционированный или нет) предъявляет такие требования к качеству информации, при выполнении которых у него не возникают сомнения в недостоверности получаемой информации. Качество получаемой информации оценивается относительным количеством правильно принятых или искаженных элементов сообщения (букв, цифр, звуков речи, элементов изображения) или значениями искажений признаков объектов.

Так как добывание информации является динамическим процессом, то для ее реализации необходима синхронизация работы всех элементов, обеспечивающих этот процесс. Необходимость функционирования органа добывания, синхронизированного с работой источника информации, составляет суть временного условия разведывательного контакта. При невыполнении его информацию не удастся получить даже в случае достаточной энергетики носителя. Действительно, если в кабинете ценного источника информации, например, руководителя фирмы, установлено закладное устройство, которое позволяет прослушивать все ведущие в нем разговоры, а кабинет пуст, то временное условие не выполнено. Злоумышленник, находящийся в припаркованной вблизи от территории фирмы машине, напрасно теряет время. Аналогичный результат наблюдается, когда в этом кабинете проводится совещание, но приемник злоумышленника неисправен или изменилась нестабилизированная частота закладного устройства и «вышла» из полосы приемника злоумышленника, в результате чего приемник не принимает сигналы закладки.

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

Способы доступа к информации можно разделить на три группы:

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

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

Скрытое проникновение имеет ряд преимуществ по сравнению с остальными, но

требует тщательной подготовки и априорной информации о месте нахождения источника, системе обеспечения безопасности, возможных маршрутах движения и др. Кроме того, скрытое проникновение не может носить регулярный характер, так как оно связано с большим риском для злоумышленника, и приемлемо для добывания чрезвычайно ценной информации.

Для обеспечения регулярного доступа к информации проводится внедрения и легализация злоумышленника путем поступления его на работу в интересующую организацию. Так как при найме на работу претендент проверяется, то злоумышленник должен иметь убедительную легенду своей прошлой деятельности и соответствующие документы. Рассмотренные способы обеспечивают скрытность добывания информации. Когда в ней нет необходимости, а цена информации очень велика, то возможно нападение на сотрудников охраны с целью хищения источника с информацией. К таким источникам относятся, например, документы, которыми можно шантажировать конкурента или вытеснить его с рынка после публикации.

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

Основными способами привлечения таких сотрудников являются следующие:

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

Инициативное сотрудничество предполагает привлечение людей, которые ищут контакты с разведкой зарубежного государства или конкурента, к сотрудничеству с целью добывания секретной или конфиденциальной информации по месту работы. Таких людей выявляют органы разведки путем наблюдения за сотрудниками и изучения их поведения, интересов, моральных качеств, слабостей, связей, финансового положения. В основе инициативного сотрудничества или предательства в подавляющем большинстве случаев лежат корыстные и аморальные мотивы, которые часто прикрываются рассуждениями о высоких целях.

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

Другие способы склонения к сотрудничеству связаны с насильственными действиями злоумышленников. Это - психическое воздействие, угрозы личной безопасности, безопасности родных, имущества, а также преследования и шантаж, принуждающие сотрудника фирмы нарушить свои обязательства о неразглашении тайны. Если в результате предварительного изучения личностных качеств сотрудника фирмы, его жизни и поведения выявляются компрометирующие данные, то возможен шантаж сотрудника с целью склонения его к сотрудничеству под угрозой разглашения компрометирующих сведений. Зарубежными спецслужбами часто создаются для приезжающих в их страну специалистов различного рода провокационные ситуации с целью получения компромата для последующего шантажа.

Выпытывание - способ получения информации от человека путем задания ему вопросов. Способы выпытывания разнообразны: от скрытого выпытывания до выпытывания под угрозой или в ходе физического или психического воздействия, - под пыткой. Скрытое выпытывание возможно путем задания в ходе беседы на конференции, презентации и или любом другом мероприятии вроде бы невинных вопросов, ответы на которые для специалиста содержат конфиденциальную информацию. Применяется скрытое выпытывание в устной или письменной форме при фиктивном наеме сотрудника конкурирующей фирмы на более высокооплачиваемую или интересную работу. Причем

приглашение доводится до сотрудника в неявной форме, не вызывающей подозрение, через знакомых, в объявлении в средствах массовой информации об имеющейся вакансии по специальности сотрудника, но с существенно более высокой заработной платой. После получения в беседе с претендентом информации ему под различными предлогами отказывают в приеме на работу. Выпытывание под пыткой характерно для криминальных элементов, которые не утруждают себя применением скрытых, требующих длительной подготовки, способов добывания информации.

Дистанционное добывание информации предусматривает съем ее с носителей, распространяющихся за пределы области физического контакта злоумышленника с источником информации. Часто рассматривается вариант, когда информации снимается за пределами контролируемой зоны (территории, помещения), но возможны иные варианты. Дистанционное добывание информации возможно в результате наблюдения, подслушивания, перехвата, сбора носителей информации в виде материальных тел (бракованных узлов, .деталей, демаскирующих веществ и др.).за пределами организации.

Наблюдение предполагает получение и анализ изображения объекта наблюдения (документа, человека, предмета, пространства и др.), а также добывание семантической информации и сигнальных признаков. В результате наблюдения добываются в основном видовые признаки объектов. Но может быть получена и семантическая информация, если объект наблюдения представляет изображение на языке общения. Например, текст или схема конструкции прибора на столе руководителя или специалиста могут быть подсмотрены в ходе их посещения. Также возможно наблюдение через окно текста и рисунков на плакатах, развешенных на стене во время проведения совещания.

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

- визуально-оптическое;
- с помощью приборов наблюдения в ИК-диапазоне;
- наблюдение с консервацией изображения (фото и киносъемка);
- телевизионное наблюдение;
- лазерное наблюдение;
- радиолокационное наблюдение;
- радиотепловое наблюдение.

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

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

Основной недостаток визуально-оптического наблюдения в видимом и ИК-диапазонах - невозможность сохранения изображения для последующего анализа специалистами или документирования результатов наблюдения. Учитывая важность документирования, в криминалистике, например, уголовное дело кроме тщательного описания места преступления содержит его фотографии. Для статической консервации (сохранения) изображения объекта его фотографируют, для динамической консервации подвижных объектов производят кино- или видеосъемку. Наблюдение объектов с одновременной передачей их изображений на любое, в принципе, расстояние осуществляется с помощью телевизионного наблюдения. Возможно так называемое лазерное наблюдение в видимом и ИК-диапазонах, которое обеспечивает возможность, кроме того, измерения с высокой точностью расстояния до объекта и его координат. Радиолокационное наблюдение позволяет получать изображение удаленного объекта в

радиодиапазоне в любое время суток и в неблагоприятных климатических условиях, когда невозможны другие способы наблюдения. Радиоэлектронное визуальное наблюдение сигналов производится на экранах осциллографов, спектроанализаторов, мониторов ПЭВМ.

Подслушивание - один из наиболее древних способов добывания информации. Подслушивание, как и наблюдение, бывает непосредственное и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов во время разговора людей и значительного затухания акустической волны непосредственное подслушивание возможно на небольшом расстоянии (единицы или в лучшем случае при отсутствии посторонних звуков - десятки метров). Поэтому для подслушивания применяются различные технические средства. Этим способом добывается в основном семантическая (речевая) информации, а также сигнальные демаскирующие признаки от работающих механизмов и машин, а также других источников звуков, например, выстрелов и взрывов.

Перехват предполагает несанкционированный прием радио и электросигналов и извлечение из них семантической информации, сигнальных демаскирующих признаков и формирование изображений объектов при перехвате телевизионных или факсимильных сигналов.

Многообразие технических средств и их комплексное применение для добывания информации порой размывает границы между рассмотренными способами. Например, при перехвате радиосигналов сотовой системы телефонной связи возможно подслушивание ведущихся между абонентами разговоров, т. е. одновременно производится перехват и подслушивание. Учитывая неоднозначность понятий «подслушивание» и «перехват», способы добывания акустической информации целесообразно относить к подслушиванию, а несанкционированный прием сигналов от других источников - перехватом.

2.5.1. Добывание информации без физического проникновения в контролируемую зону

Добывание конфиденциальной информации без проникновения в контролируемую зону осуществляется путем съема ее с носителей, распространяющихся за пределы контролируемой зоны. Под контролируемой зоной понимается физически огражденная или условно (в документах) обозначенная территория, в пределах которой обеспечивается защита информации или, по крайней мере, проводятся мероприятия по защите информации. Внешней границей контролируемой зоны является граница территории предприятия, организации государственных или коммерческих структур.

Наибольшая безопасность злоумышленника обеспечивается, когда информация им добывается вне территории интересующей его организации. За пределы территория возможен выход следующих носителей:

- людей;
- материальных носителей в виде бумажных и машинных носителей с документами и публикациями, продукции, материалов, сырья, оборудования, газообразных, жидких и твердых отходов, частиц радиоактивных излучений;
- акустических, электрических, магнитных и электромагнитных полей, в том числе в оптическом диапазоне; электрического тока, распространяющегося по проводам электропитания, телефонной сети, радиотрансляции, охранной и пожарной сигнализации.

Эти носители могут содержать семантическую и признаковую информацию, а также демаскирующие вещества.

Так как угроза привлечения злоумышленника к ответственности за противоправные действия снижается с удалением его от источника, то злоумышленника прежде всего интересуют носители с нужной ему информацией на максимально-возможном удалении

от источника.

По дальности распространения носители, выходящие за пределы контролируемой зоны, можно разделить на 3 группы:

- без ограничения расстояния (люди, переносимые или перевозимые документы, продукция, отходы и другие материальные носители);

- распространяющиеся за пределы прямой видимости (акустические волны большой мощности, радиоволны в ДВ, СВ, КВ диапазонах, электрический ток с информацией по кабелям, свет по световодам, жидкие и газообразные отходы);

- распространяющиеся в пределах прямой видимости (свет, речь, радиоволны в УКВ диапазонах, слаботочные электрические сигналы, радиоактивные излучения).

Очевидно, что чем на большее расстояние распространяется носитель, тем выше потери его энергии и тем меньшее значение принимает отношение сигнал/шум на входе приемника сигналов злоумышленника. Поэтому для обеспечения дистанционного добывания информации разведка и криминальные структуры применяют наиболее чувствительную аппаратуру для приема носителя и съема с него информации. Спецслужбы ведущих стран создают собственные научно-исследовательские организации и производственные предприятия для создания разведывательной техники с параметрами, превышающими параметры лучших образцов аппаратуры бытового и даже военного назначения, прежде всего, по чувствительности и разрешающей способности.

С другой стороны, чем меньше вес, габариты и энергопотребление средств разведки, тем проще их скрытно приблизить к источнику информации и выполнить энергетическое условие.

Требования к аппаратуре по электрическим и масса-габаритным характеристикам противоречивы. Улучшение параметров на каждом этапе развития радиоэлектроники, оптики и других прикладных областей науки и техники достигается усложнением аппаратуры до тех пор, пока не реализуются новые идеи, приводящие к скачку в методах и технологии. Но на определенном этапе технического прогресса усложнение технических решений приводит к увеличению веса и габаритов средств добывания.

Противоречие разрешается путем дифференциации средств по способам применения. Классификация наземных средств добывания информации по способам применения приведена на рис. 2.4.

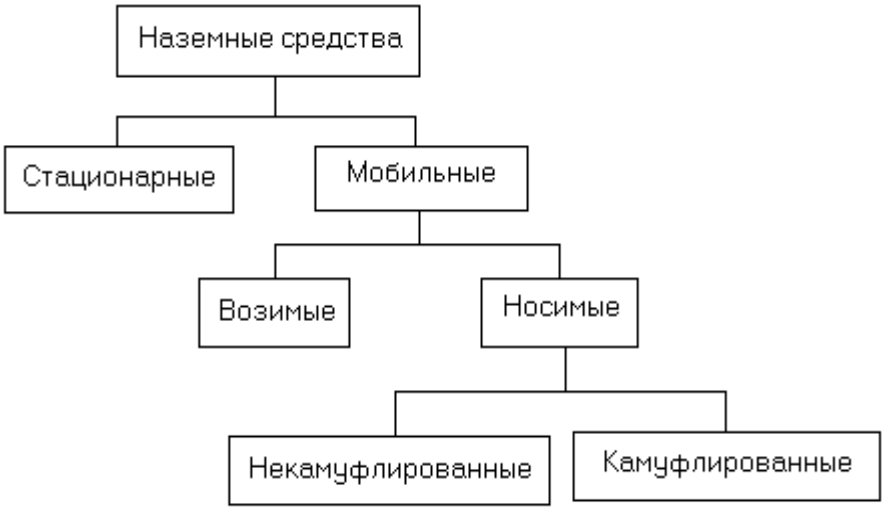


Рис. 2.4. Классификация наземных средств добывания информации.

Стационарная аппаратура размещается в отапливаемых помещениях, к ней предъявляются требования по устойчивости к механическим и климатическим воздействиям (вибрациям, ударам, температуре, влажности), пониженные по сравнению с требованиями к мобильной аппаратуре. За счет облегченных требований к условиям эксплуатации в этой аппаратуре при приемлемых (обеспечивающих перевозку в

упакованном виде) весе, габаритах и энергопотреблении реализуются в полном объеме достижения в соответствующих областях науки и техники.

Такая, в основном радиоэлектронная, аппаратура устанавливается в посольствах и консульствах зарубежных государств для добывания информации с территории посольства или консульства, рассматриваемых по международному праву как территория соответствующего государства. В принципе подобная аппаратура может быть установлена в помещении жилого дома вблизи фирмы конкурента. Однако задачи по добыванию информации проще решаются с помощью мобильной аппаратуры.

Мобильная аппаратура широко применяется органами добывания как зарубежного государства, так и коммерческих структур. К ней предъявляются более жесткие требования по размещению и функционированию в стоящем или даже движущемся автомобиле.

Существующая возимая аппаратура обеспечивает из автомобиля визуально-оптическое и телевизионное наблюдение, фотографирование, перехват радиосигналов, подслушивание с использованием закладных устройств. Например, размещаемый в автомобильной антенне эндоскоп HR 1780-S позволяет скрытно вести наблюдение из автомобиля. Те же задачи решает видеокамера PK 5045 с оптикой, вмонтированной в антенну. Вращением антенны из салона автомобиля можно на экране телевизионного приемника в салоне наблюдать и записывать на видеомагнитофон изображение субъектов и объектов вокруг машины.

Особенно широкие возможности обеспечивает возимая автоматическая аппаратура, которая записывает подслушанные звуковые сигналы и перехваченные радиосигналы в отсутствии в машине человека-оператора. В этом случае припаркованный возле фирмы автомобиль может находиться длительное время, не вызывая подозрение у службы безопасности.

Носимая некамуфлированная портативная аппаратура размещается в одежде человека и в носимых им сумках и портфелях. Например, при посещении офиса банка или другой коммерческой структуры можно положить небольшую сумку с вмонтированной в нее теле- или кинокамерой на стол и в поле ее зрения попадут изображения на экранах компьютеров сотрудников, работающих с другими посетителями.

2.4.2. Доступ к источникам информации без нарушения государственной границы

Для зарубежной разведки наиболее безопасным вариантом добывания информации является съем ее с носителей, распространяющихся за пределы контролируемой зоны государства - государственной границы. Очевидно, что в этом случае добывается только та информация, носители которого могут легально или нелегально пересекать госграницу.

Основными носителями информации через государственную границу являются:
- люди, хранящие информацию в своей памяти;
- материальные тела с информацией, переносимые или перевозимые людьми;
- электромагнитные поля в световом и радиодиапазонах.

Энергия полей-носителей с информацией на государственной границе зависит от расстояния от источником сигналов с информацией до границы. Учитывая это, государственные организации и предприятия, владеющие секретной информацией, размещаются по возможности в наиболее удаленных от границ местах. Кроме того, в приграничных районах обращается более серьезное внимание на обеспечение безопасности информации. Поэтому возможности зарубежной разведки по добыванию ценной информации в приграничной зоне без нарушения государственной границы весьма ограничены.

Из отдаленных от наземных границ районов страны границ достигают в основном радиоволны в ДВ, СВ и КВ диапазонах, а также УКВ радиорелейных и тропосферных линий связи вблизи границы. Поэтому вдоль границ бывшего СССР и стран Варшавского договора со странами НАТО располагались многочисленные станции радио и радиотехнической разведки, перехватывающих радиосигналы с семантической и признаковой информацией.

Без нарушения границы наиболее близко орган разведки может приблизиться к объекту защиты сверху, так как высота воздушного пространства государства составляет всего десятки км. Самолеты из-за разряженности воздуха не могут летать на высотах более 30-40 км. Безвоздушное пространство является нейтральным и не принадлежит ни одному из государств.

В мирное время наиболее эффективными носителями средств добывания информации сверху являются космические аппараты (КА) или разведывательные искусственные спутники Земли (ИСЗ).

Космическую разведку в полном объеме ведут два государства: Россия и США. Другие развитые в промышленном отношении страны (Япония, Китай, Франция и некоторые другие) ограничиваются довольно редкими запусками многоцелевых ракет и не ведут регулярно космическую разведку.

Параметры траектория движения КА (высота орбиты, угол ее наклонения относительно экватора Земли) определяются направлением и скоростью вывода ракеты - носителя. Для вывода КА на околоземную поверхность ему нужно при запуске сообщить первую космическую скорость у поверхности Земли не менее 7.91 км/с. При этой скорости орбита круговая. Чем выше скорость, тем больше высота орбиты. Минимальная высота ограничена тормозящим действием остатков атмосферы и составляет 130-150 км. При второй космической скорости более 11.186 км/с КА, может выйти из сферы действия тяготения Земли.

В зависимости от скорости и направления выведения КА располагаются на низких круговых, высоких эллиптических, геостационарных орбитах (см. на рис. 2.5).

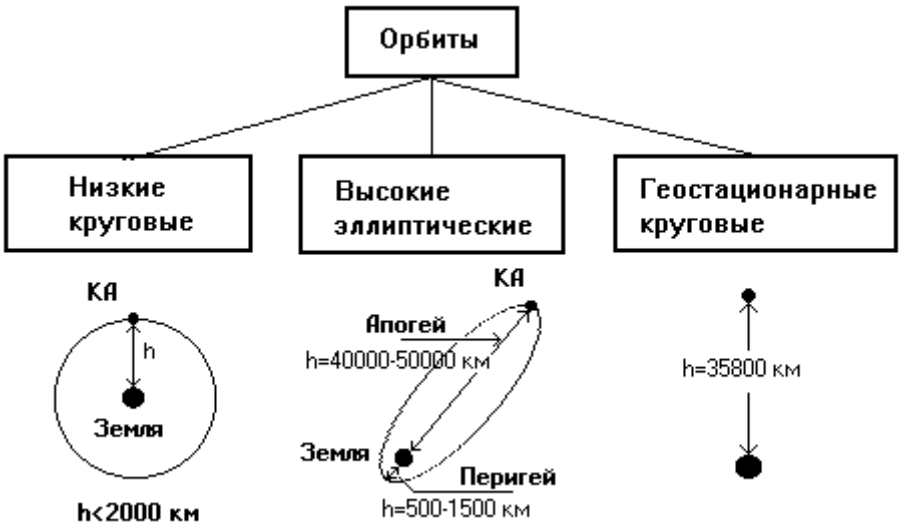


Рис. 2.5. Виды орбит разведывательных ИСЗ.

Низкие круговые орбиты - наиболее распространенные орбиты разведывательных спутников, так как они могут приблизиться к объекту на минимально-допустимое расстояние. Уменьшение высоты орбиты из-за торможения КА снижает время его существования на орбите. Противоречие между временем пребывания на орбите низколетящего КА и стремлением приблизить средства добывания информации к ее источникам решается в настоящее время путем создания маневрирующих спутников. Например, разведывательный ИСЗ США КН-12 может маневрировать на орбите по заданной программе или команде с Земли, снижаться на необходимое для решение

разведывательной задачи время до высоты 120-160 км, делать детальные фотоснимки в видимом и ближнем ИК-диапазонах с разрешением до 15 см, после чего поднимается на большую высоту, продлевая тем самым срок жизни. Передача информации на наземный пункт приема производится по радиоканалу со скоростью до 64 Мбит/с непосредственно или через спутник-ретранслятор. Этот спутник позволяет просматривать от 70 до 7000 тыс. км^2 за сутки.

Однако низкоорбитальные КА, пролетая с большой скоростью над поверхностью Земли, наблюдают объект или осуществляют перехват его радиосигналов в течение короткого времени, измеряемого минутами.

Период вращения КА вокруг Земли Тка в минутах в зависимости от высоты орбиты h можно оценить по формуле:

$$T_{ка} \approx T_0(1+h/R_з)^{3/2},$$

где $R_з$= 6372 км - радиус Земли;

T_0 = 84.4 мин - период обращения гипотетического КА по круговой орбите с радиусом, равным радиусу Земли (h=0).

В табл. 2.1 приведены некоторые значения $T_{ка}$, рассчитанные по этой формуле.

Таблица 2.1.

h, км	100	200	300	400	500	1000	5000	10000	35870	50000	100000
$T_{ка}$, мин	86,4	88,4	90,4	92,5	94.5	105	201.2	349	1440 (24 ч)	2231	5784

Из этой таблицы видно, что на малых высотах период вращения КА равен приблизительно 1,5 часа. Однако из этого не следует, что КА будет находиться над одним и тем же районом через каждые 1,5 часа. Из-за вращения Земли вокруг оси на каждом очередном витке КА будет пролетать над новым районом Земли и только через несколько суток ситуация повторится.

Возможности просмотра различных районов Земли зависят от угла наклона плоскости орбиты КА относительно плоскости орбиты.

Если КА расположен на круговой полярной орбите, то его средства могут периодически просматривать всю поверхность Земли. Например, одновременная работа 2-х спутников (с высотой орбит 1000-1400 км и наклонениями, близкими к 90^0) позволяет просматривать район земного шара с интервалом в 6 ч.

С повышением высоты орбиты, как следует из таблицы, период вращения ИСЗ увеличивается и при h около 36 тыс. км он равен периоду вращения Земли. Но скорость спутника относительно поверхности Земли равна 0, когда плоскости орбиты и экватора Земли совпадают (i= 0^0). Если ИСЗ расположен на геосинхронной орбите, то он постоянно “висит” над одним и тем же районом Земли, размеры которого определяются углом зрения средств добывания. Будучи расположенным в плоскости экватора Земли средства добывания ИСЗ не “видят” из-за кривизны Земли ее северные и южные районы (более 70 градусов широты). Это обстоятельство и большая удаленность КА от поверхности Земли существенно ограничивают возможности геостационарных спутников наблюдением ярких источников света (например, факелов ракет при их пуске) и перехватом достаточно мощных радиопередатчиков каналов связи.

Промежуточное положение занимают КА на высоких эллиптических орбитах (см. рис.2.5). Но применяются спутники на таких орбитах в основном для обеспечения связи над неудобно расположенной для геостационарных ИСЗ территорией России. Системы космической связи на эллиптических орбитах позволяют осуществлять радио и телевизионное вещание на всей территории России. Типовая орбита соответствует эллипсу с перигеем (наименьшим расстоянием до поверхности Земли - 400-460 км) и апогеем (наибольшим расстоянием - до 70000 км).

Таким образом, для добывания информации преобладают КА, на которых устанавливаются различные средства добывания (фото, телевизионного и

радиолокационного наблюдения, средства радио и радиотехнической разведки). Аппаратура современных разведывательных низкоорбитальных ИСЗ обладает высокими возможностями. Наибольшее разрешение обеспечивают ИСЗ фоторазведки. Установка на КА аппаратуры обзорной разведки обеспечивает съемку поверхности шириной до 180 км при линейной разрешении на местности 2,5-3,5 м. Опознаются объекты размером 12,5-35 м. Детальная фоторазведка обеспечивает полосу шириной 12-20 км, разрешение на местности 0,3-0,6 м, опознаются объекты размером 1,5-6 м.

Космическая разведка США имеет на вооружении разнообразные разведывательные системы: специализированные (фото, оптико-электронные, радио и радиотехнические, радиолокационные) и комплексной разведки, например, фотографирование и перехват радиотехнических сигналов. По мере прогресса в миниатюризации средств добывания доля комплексных систем возрастает.

Таким образом, космическая разведка обеспечивает наиболее близкий и безопасный для органа добывания доступ к защищаемым объектам и в силу этого обладает достаточно высокими показателями по разрешению и достоверности получаемой информации.

В то же время космическая разведка имеет ряд особенностей, которые облегчают задачу защиты информации на объекте. Кратковременность нахождения низкоорбитального ИСЗ над защищаемыми объектами, возможность точного математического расчета характеристик орбит и моментов времени пролета спутников над защищаемыми объектами позволяют применять простые, но эффективные меры по защите информации. Эти меры направлены, прежде всего, на противодействию выполнения временного условия разведывательного контакта, т. е. невозможности наблюдения за объектом в момент пролета КА на ним.

В мирное время дополнительная возможность для органов добывания государственной разведки приблизиться к защищаемым объектам обеспечивается при размещении их средств добывания на летательных аппаратах (самолетах-разведчиках, беспилотных летательных аппаратах) и кораблях, летающих (плавающих) вдоль воздушной (морской) границ.

С целью увеличения дальности видимости с самолетов-разведчиков соответствующей конструкцией добиваются подъема их на максимально-возможную высоту. Характеристики самолетов-разведчиков США приведены в табл.2.2.

Таблица 2.2.

Тип	Скорость, км/ч	Дальность полета, км	Потолок, м	Аппаратура
RC-135	1000	до 12000	15000	АФА, РРТР, РЛС БО
U-2	850	до 7000	26000	АФА, РРТР, ИК
SR-71	3300	7000	24000	То же
TR-71	740	4850	27430	То же

Примечание: АФА - авиационная фотоаппаратура, РРТР - средства радио и радиотехнической разведки, РЛС БО - радиолокационные станции бокового обзора, ИК - средства наблюдения в ИК-диапазоне.

Дальность наблюдения с самолета наземных объектов зависит от способа добывания и колеблется от 2-3 h для ИК-аппаратуры, где h-высота полета самолета, до 100-120 h для Р и РТР. При этом достигается разрешение на местности от десяти см (для фотосъемки) до метров - для радиолокационных станций бокового обзора.

Разрешение и точность определения координат наземных объектов с самолетов выше аналогичных характеристик аппаратуры ИСЗ в пропорции, соответствующей соотношению высот полетов.

Возможности добывания информации с кораблей, находящихся в нейтральной зоне возле морских границ, ограничиваются в основном перехватом радиосигналов, наблюдением берегов и их подводного рельефа.

2.6. Показатели эффективности разведки

Наиболее общим критерием эффективности разведки, включающей органы управления, добывания и обработки, является степень выполнения поставленных перед нею задач. Но этот критерий не конструктивен и не достаточно объективен, так как уровень соответствия добытой информации требуемой оценивается ее потребителем. Для более объективного определения возможностей используется группа общесистемных показателей количества и качества информации:

- полнота;
- своевременность;
- достоверность;
- точность измерения демаскирующих признаков;
- суммарные затраты на получение информации.

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

$$П_и = \frac{\sum_{i=1}^{n} \alpha_i \beta_i}{n},$$

где α_i - “вес” i-го тематического вопроса;

β_i = 1, когда количество и качество информации соответствует i-му тематическому вопросу и равно 0, когда не соответствует.

Своевременность информации является важным показателем ее качества, так как она влияет на цену информации. Если добытая формация устарела, то затраты на ее добывание оказались напрасными - она не может быть эффективно использована злоумышленником. Поэтому своевременность следует оценивать относительно продолжительности ее жизненного цикла. Если время устаревания информации существенно больше времени ее использования после добывания, то она своевременная. В противном случае она устаревшая. Достоверность информации - важнейший показатель качества информации. Она искажается в результате преднамеренного дезинформирования и под действием помех. Так как использование ложной (искаженной) информации может нанести в общем случае больший ущерб, чем ее отсутствие, то выявлению достоверности добытой информации ее пользователь уделяет большое внимание.

Для оценки достоверности используют следующие частные показатели:

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

Для количественной оценки достоверности сообщения применяется различные качественно-количественные способы и шкалы, в том числе, так как называемая схема Кента. В соответствии с ней диапазон возможных изменений достоверности разбивается на 7 интервалов и достоверность конкретной информации оценивается в шансах.
Схема Кента имеет следующий вид:

- достоверная информация (вероятность отсутствия ложной информации близка к 1);

- почти определено, что информация достоверна (9 шансов против 1-го);
- имеется много шансов, что информация достоверна (3 шанса против 1-го);
- шансы примерно равны (1 за, 1 против);
- имеется много шансов, что информация недостоверна (3 шанса за, против 1);
- почти определенно, что информация недостоверна (за 9 шансов против 1-го);
- недостоверная информация (вероятность ложной информации близка к 1).

Достоверность информации в смысле отсутствие в ней элементов дезинформации зависит от надежности источника, от степени доверия получателя к источнику. Надежность источников оценивают по шкале:

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

Количество уровней не принципиально. Семь уровней выбрано как компромисс между точностью измерения (чем больше уровней, тем точность выше) и способностью эксперта интегрально оценивать достоверность информации. Известно, что человек в среднем способен одновременно оперировать с семью цифрами.

Качество речи во время подслушивания оценивается разборчивостью. В соответствии с лингвистическим делением речи на фразы, слова, слоги и звуки существует понятие смысловой, слоговой и звуковой (формантной) разборчивости. С точки зрения защиты речевой информации наиболее наглядным является показатель смысловой разборчивости (разборчивости фраз). Однако получение объективных оценок смысловой разборчивости затруднены из-за избыточности речи. Более надежные результаты получаются при определении слоговой или звуковой разборчивости. Поэтому они получили наибольшее распространение.

Разборчивость любого вида выраженной в процентах доли принятых без искажения слуховых единиц (фраз, слов, букв, звуков) по отношению к общему количеству переданных. Избыточность письменной или устной речи снижает требования к значениям разборчивости и обусловлена различными значениями частости использования в речи букв, а также существенно меньшим количеством разрешенных грамматикой слогов, слов и фраз по отношению к возможным комбинациям слогов, слов и фраз, которые теоретически можно составить из букв алфавита. В национальных языках следующие друг за другом слова связаны между собой смыслом и синтаксисом грамматики, а последовательно расположенные буквы в пределах одного слова - правилами орфографии. Чем больше букв в алфавите и меньше словарный состав языка, тем выше избыточность языка.

Неопределенность (энтропия) появления буквы русского алфавита из 32 букв при равновероятном выборе равна $H_0 = \log 32 = 5$ бит, с учетом реальной статистики одной буквы $H_1 = 4.35$ бит, двух букв подряд $H_2 = 3.52$ бит, трех - 3.01 бит. Для латинских языков энтропия букв принимает меньшие значения: $H_0 = 4.76$ бит, $H_1 = 4.03$ бит (английский язык), $H_1 = 4.1$ бит (немецкий язык), $H_1 = 3.96$ бит (французский язык). При увеличении количества учитываемых букв энтропия стремится к предельной величине $H_{пр}$. Разность $R = 1 - H_{пр} / H_0$ названа К. Шенноном избыточностью языка. Она характеризует долю (в процентах) неиспользуемых элементов языка из потенциально возможных.

В зависимости от количества учитываемых букв и анализируемых текстов различными авторами получены отличающиеся оценки разборчивости. Например, избыточность разговорной речи в силу ее большей “вольности”, меньшей стесненности правилами стилистики и даже грамматики меньше избыточности деловых текстов (см табл. 2.3) [8].

Таблица 2.3.

	Избыточность, %	
	русского языка	французского языка
Язык в целом	72.6	70.6
Разговорная речь	72.0	68.4
Литературные тексты	76.2	71.0
Деловые тексты	83.4	74.4

Соотношения между качеством речи и количественными значениями слоговой и словесной разборчивости приведены в табл. 2.3.

Таблица 2.3.

Качество речи	Разборчивость, %	
	Слоговая	Словесная
Предельно допустимая	25-40	75-87
Удовлетворительная	40-56	87-93
Хорошая	56-80	93-98
Отличная	80-100	98-100

Искажение слогов оказывает существенно меньшее влияние на пониманиие смысла семантической информации, заключенной в предложении или фразе, чем искажение целого слова. За счет словесной избыточности слово может быть восстановлено при отсутствии части букв или слога, что наглядно иллюстрируется в игре “Поле чудес”. Поэтому, требования к словесной разборчивости, что видно из табл. 2.5, более жесткие, чем к слоговой. Предельное значение разборчивости слогов и слов, при меньших значениях невозможно понять, равно 25 и 75% соответственно.

Цифровые данные также обладают избыточностью, но в контексте конкретного сообщения. Например, если в газете в июле месяце появляется прогноз погоды в Москве о температуре 0 или 50 градусов, то читатель этому сообщению не поверит и предположит об ошибке при верстке газеты. Однако исправить, т.е. указать точные значения цифр, он не сможет. Поэтому к достоверности передачи цифровых данных предъявляются высокие требования по достоверности передачи: одна ошибка и менее на миллион цифр. В ответственных случаях для повышения достоверности цифры пишутся прописью, как, например, принято при оформлении финансовых документов. В этом случае существенно понижается вероятность искажения цифр как под воздействием помех при передаче по каналам связи, так в результате преступных действий злоумышленников. Математический аппарат для определения достоверности приема дискретных элементов достаточно хорошо разработан в теории связи. В ней получены аналитические выражения, позволяющие вычислять вероятность приема символа или слова в зависимости от метода модуляции сигнала, вида помехоустойчивого кода, от отношения сигнал/шум на входе приемника. Например, формула для оценки вероятности ошибочного приема двоичной единицы (бита) в условиях флюктуационной помехи - шума имеет вид:

$$P_{ош}=0.5[1-\Phi(kq)],$$

где q — отношение сигнал/шум;

$$\Phi(x) = \sqrt{2/\pi} \int_0^x \exp(-y^2)\,dy,$$

к=$1/\sqrt{2}$ - амплитудная модуляция;

к=1 - частотная модуляция;

к=$\sqrt{2}$ - фазовая модуляция.

Точность измерения признаков оценивается среднеквадратичным отклонением, равным величине:

$$\sigma = \sqrt{1/n\sum_{i=1}^{n}(x_i - x_{cp})^2}, \qquad \text{где } x_{cp} = 1/n\sum_{i=1}^{n} x_i$$

Кроме показателей количества и качества информации на этапе поиска и обнаружения объектов для оценки возможностей средств добывания используют такие критерии как вероятность обнаружения (выявления на фоне помех) объектов и их распознавания, определение по измеренным признакам принадлежности объекта, его назначения, функций и свойств. Вероятность обнаружения объектов определяется в результате идентификации текущей признаковой структуры, полученной при наблюдении объекта, с эталонной. Чем больше признаков текущей структуры совпадает с признаками эталонной и чем выше их информативность, тем выше вероятность обнаружения объекта. При распознавании объектов используется тот же механизм. Для достаточно достоверной оценки величины угроз безопасности информации необходимо определение возможностей и путей попадания информации к злоумышленнику.

Глава 3. Способы и средства добывания информации

3.1. Способы и средства наблюдения

3.1.1. Способы и средства наблюдения в оптическом диапазоне

В оптическом (видимом и инфракрасном) диапазоне информация разведкой добывается путем визуального, визуально-оптического, фото- и киносъемки, телевизионного наблюдения, наблюдения с использованием приборов ночного видения и тепловизоров.

Наибольшее количество признаков добывается в видимом диапазоне. Однако видимый свет как носитель информации характеризуется следующими свойствами:

- наблюдение возможно, как правило, днем или при наличии мощного внешнего источника света;
- сильная зависимость условий наблюдения от состояния атмосферы, климатических и погодных условий;
- малая проникающая способность световых лучей в видимом диапазоне, что облегчает задачу защиты информации о видовых признаках объекта.

ИК-лучи как носители информации обладают большей проникающей способности, позволяют наблюдать объекты при малой освещенности. Но при их преобразовании в видимый свет для обеспечения возможности наблюдения объекта человеком происходит значительная потеря информации об объекте.

Эффективность обнаружения и распознавания объектов наблюдения зависит от следующих факторов:

- яркости объекта;
- контраста объект/фон;
- угловых размеров объекта;
- угловых размеров поля обзора;
- времени наблюдения объекта;
- скорости движения объекта.

Яркость объекта на входе приемника определяет мощность носителя, превышение которой над мощностью помех является необходимым условием обнаружения и распознавания объекта наблюдения. Современные приемники имеют чувствительность, соответствующие мощности нескольких фотонов.

Контрастность объекта с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания. Контраст К

определяют как отношение разности яркости объекта и фона к яркости объекта или фона:

$$К= (B_о - B_ф)/B_о,\ B_о > B_ф \quad или \quad К= (B_ф - B_о)/B_ф,\ B_ф > B_о,$$

где $B_о$ и $B_ф$ — яркости объекта и фона соответственно.

Контраст, определяемый по этой формуле, называется визуальным или физиологическим. В видимом и ближнем диапазонах световых волн контраст на входе оптической системы средства добывания несколько снижается за счет яркости дымки, которую можно рассматривать как помеху. В дальних зонах инфракрасного излучения яркость дымки не оказывает существенного влияния на изменении контраста.

Значения контраста колеблется в довольно широких пределах. При К=0.08-0.1 объект почти сливается с фоном и плохо различается на фоне.

При поиске объекта его форма не играет большой роли, а имеет значение только его площадь в пределах соотношения сторон от 1:1 до 1:10.

Увеличение угловых размеров объекта в 2 раза сокращает время, необходимое для его обнаружения, в 8 раз.

Время, необходимое для обнаружения объектов светлее и темнее фона при одинаковых абсолютных значениях контраста примерно одинаковое. С увеличением яркости фона время поиска объекта наблюдателем уменьшается, так как увеличивается разрешающая способность и контрастная чувствительность глаза. Если яркость фона чрезмерно велика, то возникает дискомфорт и ослепление, ухудшающие разрешение и контрастную чувствительность глаза.

С увеличением поля обзора увеличивается и время, необходимое для поиска объекта: двукратное увеличение поля обзора повышает время поиска в 4 раза, при этом время поиска определяется не формой поля, а его угловой площадью.

Поиск движущихся объектов имеет свои особенности: движение ухудшает видимый контраст объекта, величина которого зависит не только от угловой скорости, но и от угловой размеров объекта наблюдения. Чем меньше угловой размер объекта, тем больше влияние скорости на время и вероятность обнаружения объекта. Объекты, движущиеся с малой скоростью, обнаруживаются легче, чем неподвижные, а движущиеся с большой скоростью - труднее из-за ухудшения видимого контраста.

Так как физическая природа носителя информации в оптическом диапазоне одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имею достаточно общую структуру. Ее можно представить в виде, приведенной на рис. 3.1.

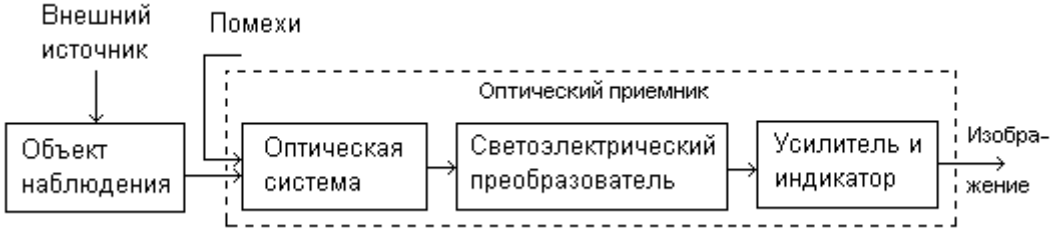


Рис. 3.1. Типовая структура средства наблюдения.

Любое средство наблюдения содержит оптический приемник, включающий оптическую систему, светоэлектрический преобразователь, усилитель и индикатор.

Оптическая система или объектив проецирует световой поток с информацией от объекта наблюдения на экран светоэлектрического преобразователя. Последний преобразует изображение на своем экране (входе) в параллельный или последовательный поток электрических сигналов, параметры которых соответствуют яркости и цвету каждой точке изображения. Размеры точки определяют разрешающую способность оптического приемника. Изменение вида носителя на выходе оптического приемника вызвано тем, что только электрические сигналы в качестве носителей информации обеспечивают возможность выполнения необходимых процедур с сигналами (усиления, обработки, регистрации и т. д.) для представления информации в форме, доступной человеку.

Возможности средств наблюдения определяются следующими характеристиками средств наблюдения:

- диапазоном частот и спектром световых лучей, воспринимаемых светоэлектрическим преобразователем;
- чувствительностью;
- разрешающей способностью;
- полем (углом) зрения.

Средства наблюдения в зависимости от назначения создаются для видимого диапазона в целом или его отдельных зон, а также для различных участков инфракрасного диапазона.

Чувствительность средства оценивается минимальным уровнем энергии светового луча, при котором обеспечивается съем информации с требуемым качеством. Применительно к свету в качестве помехи отношения сигнал/помеха выступает яркость фона на поверхности светоэлектрического преобразователя. Качество изображения зависит как от яркости света, так и контрастности принимаемого изображения. Помехи могут создавать также лучи света, попадающие на вход от других источников света, искажающие изображение или уменьшающие его контрастность. На экране светоэлектрического преобразователя при посторонней внешней засветке наблюдается ухудшение качества изображение, аналогичное варианту прямого попадания на экран телевизионного приемника яркого солнечного света.

Разрешающая способность характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые рассматриваются как отдельные. Так как изображение формируется из точек, размеры которой определяются минимальными угловыми размерами, то вероятность обнаружения и распознавания объекта возрастает с повышением разрешающей способности средства наблюдения (увеличением количества точек изображения объекта).

Поле зрения это то, что проецируется на экране оптического приемника. Угол, под которым средство «видит» предметное пространство, называется углом поля зрения. Часть поля зрения, удовлетворяющего требованиям к качеству изображения по его резкости, называется полем или соответственно углом поля изображения.

Параметры средств наблюдения определяются, прежде всего, параметрами оптической системы и оптического приемника. Но на них оказывают влияние также способы обработки.

Наиболее совершенным средством наблюдения в видимом диапазоне является зрительная система человека, включающая глаза и области мозга, осуществляющие обработку сигналов, поступающих с сетчатки глаз.

Возможности зрения человека характеризуются следующими показателями:

- глаз воспринимает световые лучи в диапазоне 0.4 - 0.76 мкм, причем максимум его спектральной чувствительности в светлое время суток приходится на голубой цвет (0.51 мкм), в темноте - на зеленый (0.55 мкм);
- порог угловых размеров, которые глаз различает как две раздельные точки на объекте наблюдения, составляют днем - 0.5-1 угл. мин., ночью - 30 угл. мин.;
- порог контрастности различимого объекта по отношению к фону составляет днем - 0.01- 0.03, ночью - 0.6;
- диапазон освещенности объектов наблюдения, к которым адаптируется глаз, чрезвычайно широк - 60-70 дБ;
- при освещенности менее 0.1 лк (в безоблачную лунную ночь) глаз перестает различать цвет.

Уникальные возможности глаз человека достигаются, в том числе благодаря совершенству его оптической системы-хрусталика, выполняющей функции объектива. Совершенство хрусталика проявляется, прежде всего, тем, что его кривизна с помощью специальных глазных мышц изменяется таким образом, чтобы обеспечить на сетчатке

глаза максимально четкое изображения объектов, расположенных на различных расстояниях от наблюдателя. Хотя ведутся исследования по созданию подобных искусственных объективов, но приблизиться к возможностям хрусталика глаза пока не удается.

Объективы

Объектив в силу постоянства кривизны поверхностей линз и оптической плотности стекла объективы проецируют изображения с различного рода погрешностями. Наиболее заметными из них являются следующие:

- сферическая аберрация, проявляющаяся в отсутствии резкости изображения на всем поле зрения (оно резко в центре или по краям);
- астигматизм - отсутствие одновременной резкости на краях поля изображения для вертикальных и горизонтальных линий;
- дисторсия - искривление прямых линий;
- хроматическая аберрация - появление цветных окантовок на границах световых переходах, вызванных различными коэффициентами преломления линз объектива спектральных составляющих световых лучей.

С целью уменьшения погрешностей объективов они выполняются из большого (до 10 и более) количества линз с различной кривизной поверхностей. Все или отдельные группы линз склеиваются между собой.

Качество объективов описываются большим количеством параметров. Для целей оценки возможностей средств наблюдения основными из них являются: фокусное расстояние, угол поля зрения и изображения, светосила, разрешение, частотно-контрастная характеристика.

По величине фокусного расстояния объективы делятся на короткофокусные, с фокусным расстоянием F, меньшим длины диагонали кадра поля изображения d, нормальные или среднефокусные ($F \approx d$), длиннофокусные и телеобъективы с $F>d$, а также с переменным фокусным расстоянием.

Объектив с переменным фокусным расстоянием (панкратический) представляют собой сложную оптическую систему, в которой предусмотрена возможность смещения оптических компонентов, за счет чего изменяется величина фокусного расстояния. Величину фокусного расстояния изменяют дискретно или плавно.

Дискретное изменение фокусного расстояния достигается применением афокальных насадок, уменьшающих или увеличивающих фокусное расстояние в два раза. Плавное изменение величины фокусного расстояния осуществляется перемещением отдельных компонент вдоль оптической оси по линейному или нелинейному закону. В зависимости от способа коррекции абберации их подразделяют на вариообъективы и трансфокаторы.

Вариообъективы представляют собой единую оптическую схему, в которой изменение фокусного расстояния осуществляется непрырывным перемещением одного или нескольких компонентов вдоль оптической оси.

Трансфокаторы состоят из афокальной насадки с переменным, плавным увеличением и объектива с постоянным фокусным расстоянием.

Сложность оптической конструкции объективов с переменным фокусным расстоянием вызвана, прежде всего, тем, что при изменении фокусного расстояния должно автоматически сохраняться положение плоскости резкого изображения наблюдаемого объекта. Добиваются этого путем оптической компенсации (при линейном перемещении компонентов) и механической (при нелинейном). В первом случае достигают кратности изменения фокусных расстояний не более 3, во втором - 6-7.

По углу поля зрения (изображения) различают узкоугольные объективы, у которых величина угла не превышает 30 град., среднеугольные (угол в пределах 30 - 60 град.),

широкоугольные с углом более 60 град. и, наконец, - с переменным углом изображения у объективов с переменным фокусным расстоянием.

Чем больше фокусное расстояние F объектива, тем больше деталей объекта можно рассмотреть на его изображении, но тем меньше угол поля зрения. Поэтому для обнаружения объекта используют короткофокусные объективы, а для распознавания - длиннофокусные. Размеры объекта h на изображении определяются в зависимости от размеров реального объекта H, расстояния от него до объектива L и фокусного расстояния объектива F по соотношению $h=F \cdot H / L$.

Светосила характеризует способность объектива создавать освещенность в поле кадра в соответствии с яркостью объекта. На светосилу объектива влияют следующие факторы:

- относительное отверстие объектива;
- прозрачность (коэффициенты пропускания, поглощения, отражения) линз;
- коэффициент увеличения (масштаб получаемого изображения);
- коэффициент падения освещенности к краю кадра.

Светосила без учета реальных потерь света в линзах оценивается величиной геометрического относительного отверстия, равного к=D/F, где D-диаметр входного отверстия объектива (апертура), F-фокусное расстояние, и обозначается в виде 1: к. Эффективное относительное отверстие объектива меньше геометрического на величину потерь света в его линзах. По величине относительного отверстия объективы делятся на сверхсветосильные, у которых 1: к>1:2, светосильные (1: к=1.28-1.4) и малосветосильные с 1: к>1.4. Чем больше светосила объектива, тем выше чувствительность средства наблюдения. Однако при этом растут искажения изображения и для их уменьшения усложняют конструкцию светосильных объективов, что естественно приводит к их удорожанию.

Свет, падающий на линзу и проходящий через нее, отражается и поглощается. Количество поглощенного света зависит от толщины стекла (в среднем 1-2% на 1 см толщины). Чем больше отражающих поверхностей имеет объектив, тем больше потери света. В объективах из 5-7 линз потери света на отражение могут составлять 40-50%. Уменьшают потери света просветлением линз.

Просветлением называются способы уменьшения отражения света от поверхности стекла путем нанесения на него тонкой пленки с коэффициентом преломления меньше преломления стекла линзы. Толщина просветляющей пленки должна составлять 1/4 длины волны падающего на линзу света. В этом случае отраженные лучи света в силу противоположности фаз с падающими компенсируются и, следовательно, отражение света отсутствует. Первоначально объективы просветляли для желто-зеленой части спектра, к которой наиболее чувствителен глаз человека. Просветленный объектив в отраженном свете приобретал сине-фиолетовый оттенок и назывался «голубой» оптикой. Современные технологии просветления оптики позволяют наносить на поверхность линзы 12-14 слоев просветляющих пленок и перекрывать тем самым весь спектр видимого диапазона света. Такую оптику маркируют индексами МС - многослойное покрытие. Объективы МС в отраженном свете не меняют цвет. В настоящее время все объективы просветляются.

Способность объектива передавать мелкие детали изображения оценивается разрешающей силой. Она выражается максимальным числом N штрихов и промежутков между ними на 1 мм поля изображения в его центре и по краю. Наиболее высокую разрешающую силу имеют объективы для микрофотографирования в микроэлектронике. Она достигает 280-440 линий на мм по центру и 260-400 линий на мм по краю кадра.

Так как одним из основных факторов, определяющих вероятность обнаружения и распознавания объектов, является контрастность его изображения по отношению к фону, то важной характеристикой объектива как элемента средства наблюдения является его частотно-контрастная характеристика. Она служит мерой способности объектива передавать контраст деталей объекта и измеряется отношением контрастности деталей

определенных размеров на изображении и на объекте. Уменьшение контраста мелких деталей на изображении вызвано тем, что в результате различных аберраций объектива на изображении размываются границы деталей наблюдаемых объектов.

Для количественной оценки частотно-контрастной характеристики в качестве исходного объекта используется эталонный объект наблюдения - мира в виде черно-белых линий с уменьшающейся шириной, нанесенных, например, тушью на белой бумаге. По результатам измерений контрастности линий на проецируемом объективом изображении строится зависимость контраста К=f(n) количества линий в 1 мм. Эта зависимость определяет частотно-контрастную характеристику объектива.

В связи с большими техническими проблемами создания универсальных объективов с высокими значениями показателей, оптическая промышленность выпускает широкий набор специализированных объективов: для фото и киносъемки, портретные, репродукционные, проекционные, для микрофотографирования и т. д.

Для добывания информации применяются в основном объективы трех видов: для аэрофотосъемки, широкого применения (фото, кино и видеосъемки с использованием бытовых и профессиональных камер) и для скрытой съемки.

Объективы широкого применения разделяются в соответствии с размерами фотоаппаратов: для малоформатных и миниатюрных, среднеформатных и крупноформатных камер. Для скрытого наблюдения используются:

- телеобъективы с большим фокусным расстоянием (300-4800 мм) для фотографирования на большом удалении от объекта наблюдения, например, из окна противоположного дома и далее;
- так называемые точечные объективы для фотографирования из портфеля, часов, зажигалки, через щели и отверстия. Они имеют очень малые габариты и фокусное расстояние, но большой угол поля зрения.

Например, объектив фотоаппарата, вмонтированного в корпус наручных часов, имеет размеры 7.5 мм с апертурой 2.8 мм. В миникамерах фирм Hitachi, Sony, Philips, Ockar используются объективы диаметром 1-4 мм и длиной до 15 мм.

Визуально-оптические приборы

Для визуально-оптического наблюдения применяются оптические приборы, увеличивающие размеры изображения на сетчатке глаза. В результате этого повышается дальность наблюдения, вероятность обнаружения и распознавания мелких объектов. К визуально-оптическим приборам относятся бинокли, зрительные трубы, перископы, стереотрубы, теодолиты. Для наблюдения за объектами наиболее распространены бинокли. Бинокль (от лат. bini-пара и oculus - глаз) - оптический прибор из двух параллельных соединенных между собой зрительных труб. В зависимости от оптической схемы зрительной трубы бинокли разделяются на обыкновенные (галилеевские) и призменные.

Зрительная труба призменного бинокля состоит из объектива, обращенного в сторону объекта наблюдения, системы призм, оборачивающей изображение, и окуляра - объектива, обращенного к зрачку глаза. В обыкновенном бинокле призмы отсутствуют, оптические оси объектива и окуляра трубы совпадают, расстояние между центрами объективов и центрами окуляров зрительных труб одинаково и равно 65 мм (среднее расстояние между зрачками глаз наблюдателя). Бинокли этого типа просты по устройству, дают прямое изображение предметов, обладают высокой светосилой, однако имеют малое поле зрения и не позволяют устанавливать углоизмерительную сетку. Наиболее распространены призменные бинокли. Они обладают сравнительно большим полем зрения и повышенной стереоскопичностью за счет увеличения расстояния между центрами объективов труб. В призменных биноклях устанавливают углоизмерительную сетку в фокальной плоскости объектива и окуляра. Зрительные трубы у призменных

биноклей шарнирно закреплены на общей оси, что позволяет подбирать расстояние между окулярами по базе глаз наблюдателя (от 54 до 74 мм). Объективы и призмы оборачивающей системы закреплены в зрительных трубах неподвижно, а окуляры могут выдвигаться для установки по силе зрения наблюдателя. Для этого на окулярных трубах наносятся диоптрийные шкалы. По увеличению (кратности) наиболее совершенные бинокли военного назначения условно разделяются на две группы: среднего увеличения (6-8 кратные, поле зрения 8-5) и большого увеличения (кратность более 10, поле зрения 5-2). Например, бинокль Б-6 имеет увеличение 6 при угле поля зрения 8.5 градусов, БП-8 - увеличение 8 при угле поля зрения-7 град., Б-15 - увеличение 15, угол поля зрения - 4 град.. Созданы широкоугольные бинокли с углом зрения до 70 и более градусов.

Чтобы улучшить наблюдение при тумане, ярком солнечном освещении или зимой на фоне снега, на окуляры бинокля надеваются желто-зеленые светофильтры. В некоторых биноклях для обнаружения действующих инфракрасных приборов ночью применяют специальный экран, чувствительный к инфракрасным лучам.

В последнее время применяются так называемые панкратические бинокли, плавно изменяющиеся увеличение в значительных пределах (от 4 до 20 и более). При этом в обратно пропорциональной зависимости изменяется величина поля зрения. Такие бинокли наиболее удобны для наблюдения: позволяют производить поиск объектов при большом поле зрения, но малом увеличении, и изучение объекта - при большом увеличении. Например, панкратический бинокль фирмы Tasko (США) имеет увеличение 8-15, угол зрения 6.0-3.6 градусов и диаметр входного зрачка 5-2.3 мм. У панкратических зрительных труб увеличение может изменяться в еще больших пределах. Например, кратность увеличения зрительной трубы фирмы Swiff (Великобритания) составляет 6-30 при угле зрения 7.5-1.3 градусов.

На базе волоконно-оптических световодов созданы разнообразные типы технических эндоскопов для наблюдения через малые отверстия диаметром 6-10 мм. Типовой технический эндоскоп состоит: из окулярной части, через которую проводится наблюдение, рабочей части в виде волоконно-оптического кабеля длиной 600-1500 мм, дистальной части, содержащей объектив, и осветительного жгута для подсветки объекта наблюдения. Эндоскопы комплектуются сетевыми или аккумуляторными осветителями с источниками света - галогенными лампами мощностью 20-150 Вт. В эндоскопе обеспечивается возможность отклонения дистальной части на 180 градусов в вертикальной и горизонтальной плоскостях. Угол поля зрения объектива составляет 40-60^0, фокусировка объектива обеспечивает наблюдение как вблизи (от 1 мм и далее), так и “ в бесконечности” (на расстоянии более 5 м).

Фото- и киноаппараты

Визуально-оптическое наблюдение, использующее такой совершенный оптический прибор, как глаз, является одним из наиболее эффективных способов добывания, прежде всего, видовой информации. Однако оно не позволяет регистрировать изображение для последующего изучения или документирования результатов наблюдения. Для этих целей применяют фотографирование и киносъемку с помощью фото и киноаппаратов.

Фотографический аппарат представляет собой оптико-механический прибор для получения оптического изображения фотографируемого объекта на светочувствительном слое фотоматериала.

Все фотоаппараты состоят из светонепроницаемого корпуса с закрепленным на его передней стенке объективом, устройства для размещения или фиксации светочувствительного материала, расположенного у задней стенки корпуса, и затвора.

Так как светочувствительный материал обеспечивает получение качественного фотографии при строго дозированной световой энергии, проецируемой на светочувствительный материал, то затвор пропускает в течение определенного времени

(времени экспозиции или выдержки) световой поток от фотографируемого объекта. Указанные части фотоаппарата являются основными. По мере конструктивного развития фотоаппарат “обрастал” различными узлами и механизмами, которые облегчали и автоматизировали процесс съемки, позволяли расширить возможности применения фотоаппарата, улучшить его технические параметры. Эти узлы и механизмы называют вспомогательными. К ним относятся:

- видоискатель для определения границ поля изображения;
- дальномер для ручного или автоматического определения расстояния до объекта съемки;
- фокусировочный механизм для совмещения фокальной плоскости объектива с плоскостью расположения светочувствительного материала;
- механизм, транспортирующий фотопленку на один кадр и точной установки ее против кадрового окна фотоаппарата;
- экспонометрический узел, предназначенный для определения экспозиционных параметров (выдержки и диафрагмы) в соответствии со светочувствительностью используемого фотоматериала и яркостью объекта.

Профессиональные фотоаппараты известных фирм (Nicon, Canon, Kodak, Contax, Pentax, Зенит) представляют собой сложнейшие оптико-электо-механические устройства, автоматически учитывающие все изменения в освещенности объекта во время фотосъемки.

Размер используемого в них светочувствительных материалов положен в основу условного деления всех фотоаппаратов на несколько групп. В настоящее время по этому признаку (по размерам получаемых негативов) выделяют пять групп: микроформатные, полуформатные, мало, средне и круноформатные. Фотоаппараты применяют различные типы светочувствительных материалов: фотопластинки, плоские и рулонные фотопленки.

Другим важным признаком классификации является назначение фотоаппарата. По этому признаку они делятся на общие и специальные.

От способов обеспечения резкого изображения на светочувствительном материале (наводки на резкость) зависит конструктивное решение почти всего фотоаппарата. По этому признаку модели, используемые для добывания информации, можно разделить на следующие группы:

- с наводкой на резкость по изображению на экране, которое проецируется объективом фотоаппарат с помощью встроенных в него подвижному и неподвижному зеркал (у так называемых зеркальных или SLR- фотоаппаратов);
- с наводкой по монокулярному дальномерному устройству (у дальномерных фотоаппаратов), механически связанному с объективом фотоаппарата;
- с неподвижным жестковстроенным объективом, сфокусированным на гиперфокальное расстояние;
- автофокусирующие (с помощью устройства автоматической фокусировки).

По технической оснащенности фотоаппараты можно разделить на следующие классы: простой, средний, высокий.

По показателям оснащенности фотоаппарата встроенными экспонометрами, а также по степени автоматизации установки экспозиционных параметров фотоаппараты делят на три группы: с ручной установки, с полуавтоматической и с автоматической установкой экспозиции.

Повышение технической оснащенности расширяет возможности фотоаппаратов, но усложняет возможность их миниатюризации.

Микроформатные фотоаппараты имеют более простую конструкцию и заряжаются узкой пленкой шириной 8-16 мм. Одна из особенностей ряда ранних микроформатных фотоаппаратов - горизонтальная компоновка аппарата с объективом, утопленным в корпусе. Корпус таких моделей состоит из двух частей, одна из которых подвижная.

Перед съемкой фотоаппарат телескопически раздвигается, открывая объектив и видоискатель. Одновременно производится транспортирование пленки и взвод затвора. Таким образом, выдвижная часть корпуса является одновременно защитным кожухом, рычагом взвода и протяжки пленки для следующего кадра (“Минокс”, “Агфаматик-4008”, “Киев-30”).

Более новые модели имеют традиционную форму. Мировыми лидерами среди производителей таких фотоаппаратов являются АО “Красногорский завод” и немецкая фирма “Robot”.

Например, фотоаппарат “МФ-1” (Красногорский завод) представляет полуавтомат с пружинным приводом, имеет светосильный объектив с F=2.8, размер кадра 18х24 мм. Конструкция фотоаппарата предполагает дистанционное управление, а пружинный привод дает возможность работать в любых климатических условиях. Недостаток - относительно большой шум при перемотке. Фотоаппарат “Robot-SC electronic” менее шумящий и при небольших габаритах работает с использованием стандартной пленки 35 мм. Параметры некоторых микроформатных фотоаппаратов приведены в табл. 3.2.

Таблица 3.2.

Наименование	Габариты, мм	Вес, г	Примечание
“Minox-C2	122х28х16	102	F=15 мм
PK 1570-SS (в зажигалке)	26х16х55	40	Негатив 8х11 мм
OVS-1	*	36	Пленка шириной 9.5 мм
PK 415	30х18х80	50	Кассета 12, 24, 36 кадров
PK 365	28х52х68	165	Негатив 14х21 мм
PK 785-S	120х50х38	180	F=24 мм, негатив 13х17 мм

Возможности добывания информации путем фотографирования определяются, как параметрами фотоаппаратов, так характеристиками (спектральным диапазоном, чувствительностью, разрешающей способностью) светочувствительных материалов, на которые проецируется объективом изображение наблюдаемого объекта.

Светочувствительные материалы (фотокинопленка, фотопластины, фотобумага) представляют собой тонкую желатиновую пленку, содержащую светочувствительные вещества на целлулоидной пленке, стеклянной пластине или плотной бумаге.

Для фотосъемки наиболее широко применяются материалы, у которых в качестве светочувствительного слоя используются мельчайшие кристаллы галгенида серебра (AgBr, AgCl, AgI), взвешенные в растворе желатины. Этот раствор, называемый эмульсией и нанесенный тонким слоем на подложку, после высыхания образует тонкий, сравнительно твердый и гибкий слой. Галоидное серебро является непосредственным приемником световых лучей. Поэтому от особенностей строения, размеров, количества и пространственного распределения в слое зерен галоидного серебра существенно зависит качество получаемого изображения.

В момент экспонирования под действием квантов света в микрокристаллах галогенида серебра происходит образование металлического серебра, которое осаждается на центрах светочувствительности (центрах скрытого изображения), увеличивая их размер. Таким образом, в результате фотографирования в светочувствительном слое возникает скрытое изображение. Для превращения его в видимое изображение необходима химическая обработка светочувствительного слоя, включающего проявление, фиксирование, промывку и сушку.

При проявлении происходит превращение невидимого изображения в видимое путем воздействия на микрокристаллы галогенидов серебра со следами скрытого изображения химическими веществами проявителя. В результате этого воздействия экспонированные микрокристаллы галогенидов серебра восстанавливаются до металлического серебра, образуя видимое изображение.

Кристаллы, не подвергшиеся действию света, остаются в светочувствительном слое. Для удаления из эмульсионного слоя неэкспонированных и соответственно невостановленных в процессе проявления кристаллов галогенида серебра производится фиксирование, в ходе которого галогенид серебра под действием некоторых химических веществ превращается в несветочувствительное, прозрачное, легко растворимое соединение.

После промывки с целью удаления из светочувствительного слоя продуктов реакции проявления и фиксирования и последующей сушки получается негативное изображение. В негативном изображении степень почернения его элемента пропорциональна яркости исходного изображения на светочувствительном слое. Для получения позитивного (прямого) изображения необходимо провести позитивный процесс, включающий фотопечать, проявление, фиксирование и сушку. Позитивная фотопечать проводится путем экспонирования фотоматериала через негатив. При проявлении позитивного фотоматериала на нем получается изображение, обратное по яркости изображению негативу.

Так как энергия фотонов снижается с увеличением длины волны, то для формирования спектрального диапазона светочувствительного материала в слой вводят добавки-сенсибилизаторы. Черно-белые фотопленки по спектральной чувствительности делятся на категории, указанные в табл. 3.3.

Таблица 3.3.

Спектральная характеристика пленки	Зона сенсибилизации, мкм	Зона спектра, к которой чувствительна пленка
Несенсибилизированная	до 0.50	Ультрафиолетовая, фиолетовая, синяя
Ортохроматическая	0.58	Зеленая, желтая
Изоортохроматическая	0.60	Синяя, желтая, зеленая
Изохроматическая	0.64	Синяя, зеленая, оранжевая, оранжево-красная
Панхроматическая	0.68 - 0.70	Синяя, зеленая, красная
Изопанхроматическая	0.70	Синяя, зеленая, красная
Инфрахроматическая	0.90	Инфракрасная

В настоящее время широко применяется, в особенности из космоса, «многозональная съемка», которая предусматривает одновременное (синхронное) фотографирование одного и того же участка земной поверхности или объекта в различных (обычно 4-6) узких (0.04-0.10 мкм) зонах спектра на фотопленки с различными спектральными характеристиками. Информативность многозональных снимков зависит от информативности зон спектра, в которых производят съемку. Но в любом случае она выше, чем черно-белых цветных фотографий.

В современных способах цветной фотосъемки цветовыделение осуществляется использованием многослойных фотоматериалов, имеющих на одной подложке три эмульсионных слоя. Каждый из слоев чувствителен к лучам одного из основных цветов: синего, зеленого и красного. При съемке в каждом из трех эмульсионных слоев образуется скрытое изображение. Фотохимическая обработка цветных материалов сложнее, чем черно-белых и состоит из следующих операций: проявление, отбеливание, фиксирование, промывка, сушка и ряда промежуточных операций, способствующих повышению качества цветного изображения. Отбеливание, отсутствующее при обработке черно-белых материалов, предназначено для перевода металлического серебра в центрах скрытого изображения, снижающего яркость красителей слоев, в его комплексную соль.

Многослойные цветные фотопленки существенно уступают черно-белым по разрешающей способности, что усугубляется также значительным влиянием воздушной дымки в атмосфере на контраст изображения в сине-фиолетовой зоне спектра. Поэтому цветная фотосъемка применяется при невысоких требованиях по разрешению и большой информативности такого демаскирующего признака как цвет. В интересах разведки

цветная космическая и воздушная съемка широко не применяется. Для этих целей более распространена фотосъемка на основе спектрозональных аэрофотопленок, имеющих 2-3 эмульсионных светочувствительных слоя. В отличии от цветных пленок, к которым предъявляются требования по идентичности в калориметрическом отношении изображения и оригинала, на спектрозональных аэрофотопленках объекты отображаются в условных цветах, не соответствующих привычному цвету объектов.

Технология съемки и фотохимической обработки спектрозональной пленки не отличается от цветной. Но информативность спектрозональных снимков значительно выше, чем цветных по следующим причинам:

- используются наиболее информативные с точки зрения возможностей обнаружения и распознавания объектов зоны спектра;
- зоны смещены в область больших значений длин волн, вследствие чего уменьшается отрицательное влияние воздушной дымки на контраст оптического изображения;
- двухслойные спектрозональные аэрофотопленки имеют более высокую (примерно в 2 раза) разрешающую способность, чем многослойные цветные пленки.

Чувствительность фотоматериалов измеряется в России в условных единицах ISO (до недавнего времени в единицац ГОСТа), в США и многих других странах- в единицах ASA, в Германии - в DINax. Перерасчет чисел светочувствительности, определенных по разным сенсиметрическим системам, сложен, так как в каждой системе используются разные критерии светочувствительности. Ситема ISO практически идентична системе ASA. В единицах DIN чувствительность приблизительно равны десятикратному значению десятичного логарифма значений светочувствительности в единицах ISO. Например, широко применяемая для бытовой съемки пленка имеет чувствительность 100, 200 и 400 ед. ISO соответствует чувствительности 21, 24 и 27 ед. DIN. В зависимости от назначения чувствительность фотоматериалов колеблется в широком диапазоне - от единичных значений до тысяч. Фирма «Кодак» выпускает специальную фотопленку, значения чувствительности которой достигают 10 тысяч единиц. Такая пленка позволяет проводить фотосъемку при освещенности, оцениваемой человеком как темнота. Однако она требует специальной обработки за 10-12 часов перед фотосъемкой. Разработана монохроматическая пленка переменной чувствительности, величина которой зависит от длительности ее проявления.

Разрешающая способность, так же как для объективов, оценивается в линиях на один мм и достигает для специальных пленок, используемых для микрофотографирования, значений в 200-300 линий/мм. Способность фотоматериала раздельно с заданным контрастом воспроизводить мелкие близко расположенные детали изображения определяется структурными свойствами фотографических материалов. Зернистая структура фотографической эмульсии вызывает рассеяние света в слое при экспонировании и ограничивает возможность воспроизведения мелких деталей и резкость изображения. Причем чем выше чувствительность фотоматериала, тем больше зернистость эмульсии. Разрешающая способность аэрофотопленок достигает 200 и более лин/мм, пленки широкого применения имеют разрешение менее 100 лин/мм.

В настоящее время в результате достижений в микроэлектронике развивается принципиально новое направление в фотографировании - цифровое электронное фотографирование. Цифровой фотоаппарат представляет собой малогабаритную цветную телевизионную камеру на ПЗС, электрические сигналы с выхода которой записываются не на магнитную ленту, как в видеокамере, а преобразуются в цифровой вид и запоминаются полупроводниковой памятью фотоаппарата. Информация, содержащаяся в памяти, может просматриваться на экране телевизора, цветное изображение регистрируется на бумаге с помощью специального принтера. Цифровой фотоаппарат также сопрягается с ПЭВМ. Отснятое изображение может отображаться на экране дисплея, редактироваться с помощью графических редакторов и выводиться на печать принтером.

Сравнительные характеристики цифровых фотоаппаратов приведены в табл 3.4

Таблица 3.4

Модель	Разрешение, точки	Емкость ОЗУ, МБайт	Кол. кадров	Габариты, см	Масса, г
Agfa ePhoto 307	640x480/ 320x240	2	36/72	76x140x38	370
Apple Quik-Take 150	640x480/ 320x240	1	16/32	56x135x155	455
Canon Power-Shot 600	832x608/ 320x240	1	4/36	90x157x58	625
Casio QV-10- Aplus	480x240	2	96	65x130x40	200
Epson Photo PS	640x480/ 320x240	1	16/32	90x165x50	65
Kodak DC20	493x373/ 320x240	1	8/16	60x100x30	120
Kodak DC40	756x504	4	48/99	155x155x135	455
Kodak DC50	756x504	1	7/22	60x110x150	625
Olympus D-200l	640x480/ 320x240	2	20/80	145x70x45	310
Ricoh RDC-2	768/576	2	9/38	9/38	310

Примечание. В столбцах 2 и 4 в числителе указаны максимальные значения, в знаменателе - минимальные.

Отснятые кадры могут просматриваться на экране телевизора, записываться на видеомагнитофон, передаваться на IBM-совместимые компьютеры. В процессе просмотра изображения на ПЭВМ можно увеличивать отдельные части кадра, одновременно наблюдать на дисплее 1, 4 или 9 кадров изображения с целью выбора лучшего для вывода на печать.

Разрешение изображения цифрового фотоаппарата определяется разрешением его светоэлектрического преобразователя. Но с увеличением разрешения уменьшается при ограниченном объеме памяти количество кадров. Компромисс между разрешением и количеством кадров достигается введением возможности изменения оператором показателей разрешения запоминаемого кадра. Если использовать карты памяти стандарта PCVIA, то количество кадров может существенно увеличено. Для дополнительной памяти объемом 16 Мб количество кадров пропорционально возрастает и составляет сотни снимков.

Изображение с разрешением 640x480 соответствует качеству телевизионного изображения, но уступает возможностям фотопленок. Однако цифровое фотографирование не связано с химической обработкой светочувствительных материалов, что резко улучшает потребительские свойства цифровых фотоаппаратов, обладает большой оперативности просмотра изображений и гибкостью редактирования изображения на ПЭВМ.

Учитывая перспективы миниатюризации радиоэлектронных элементов, прежде всего «памяти», и повышения разрешения ПЗС, у цифровых фотоаппаратов большое будущее.

Информация о движущихся объектах добывается путем кино и видеосъемки с помощью киноаппаратов и видеокамер. При киносъемке изображение фиксируется на светочувствительной кинопленке, при видеозаписи - на магнитной пленке.

Под киносъемкой понимают процесс фиксации серии последовательных изображений (кадров) объекта наблюдения через заданные промежутки времени, определяемые частотой кадров в секунду. Каждый кадр кинофильма содержит единичный изображение объекта и соответствует состоянию объекта в момент съемки. Число кадров

колеблется от единиц кадров в минуту и даже часов для съемки медленно текущих процессов до сотен тысяч в секунду для сверхскоростной специальной съемки, например, для наблюдения электрического разряда или полета пули.

Устройство кинокамеры близко к устройству фотоаппарата с той принципиальной разницей, что в процессе киносъемки пленка скачкообразно продвигается с помощью грейферного механизма перед кинообъективом на один кадр. Закрытие объектива на время продвижения кинопленки осуществляется заслонкой (обтюратором), вращение которой перед объективом синхронизировано с работой грейфера. Внутри и вне помещений киносъемка движущихся людей производится на 8 и 16-мм пленку с частотой 8-32 кадра в секунду.

Средства телевизионного наблюдения

Видеокамера является средством регистрации движущихся изображений с помощью средств телевизионного наблюдения. Схема средств телевизионного наблюдения показана на рис. 3.4.

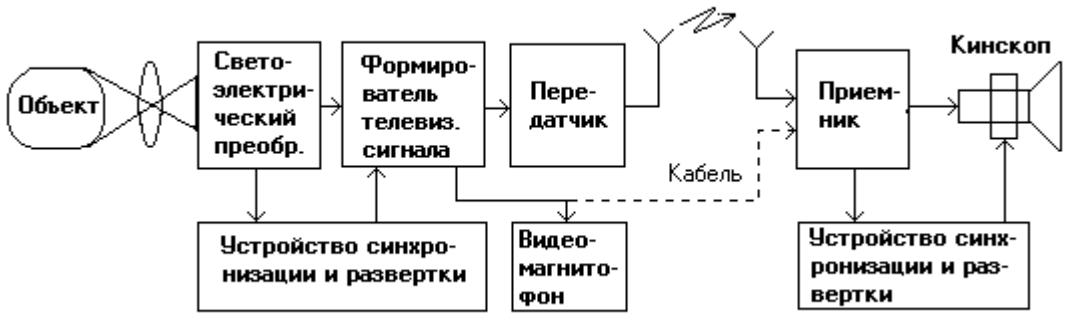


Рис. 3.4. Схема средств телевизионного наблюдения.

При телевизионном наблюдении изображение объективом проецируется не на светочувствительный слой фото или кинопленки, как при фото или киносъемке, а на фотокатод вакуумной передающей трубки или твердотельного преобразователя. Фотокатод содержит вещества, из атомов которого кванты световой энергии выбивают электроны, количество которых пропорционально энергии света (яркости элемента изображения). На фотокатоде образуется изображение Q(x,y,t) в виде электрических зарядов, эквивалентное оптическому B(x,y,t) изображению, где Q и B - значения соответственно величины зарядов и яркости в точками с координатами x, y в момент времени t.

В вакуумных телевизионных передающих трубках производится считывание величины заряда с помощью электронного луча трубки, перемещающегося по горизонтали и вертикали под воздействием магнитного поля. Это поле создается отклоняющими катушками, надеваемыми на горловину телевизионной трубки.

За время развития телевидения разработано много типов передающих телевизионных трубок, отличающихся чувствительностью фотокатода и разрешающейся способностью. Появление достаточно простых ТВ-трубок типа “видикон” позволило создать компактные телекамеры. Миниатюрные видиконы с диаметром до 15 мм обеспечивают четкость 400-600 линий. На основе видикона разработаны различные варианты телевизионных передающих трубок: плюмбикон, кремникон, суперкремникон, секон, обеспечивающих качественное светоэлектрическое преобразование в широком диапазоне длин волн света и освещенности. В начале 70-х годов был открыт и реализован новый принцип построения безвакуумных, твердотельных преобразователей ”свет-электрический сигнал”, т. н. приборов с зарядовой связью (ПЗС).

В основу таких приборов положены свойства структуры металл-окисел-

полупроводник, называемой МОП-структурой (рис. 3.5).

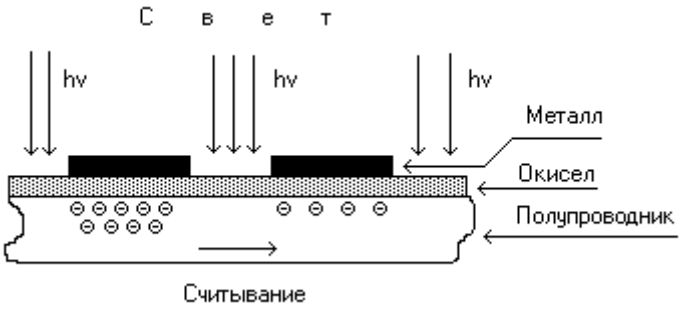


Рис. 3.5. Схема фрагмента ПЗС.

Фотокатод или мишень ПЗС представляет матрицу из ячеек с МОП-структурами. Размеры каждой ячейки соответствуют размерам элементам изображения. Разрешающая способность ПЗС определяется количеством ячеек, размещающихся в поле изображения фотокатода.

Считывание зарядов, образующихся в каждой ячейке ПЗС под действием света изображения, попадающего на светочувствительную поверхность ячейки, производится путем последовательного перекачивания зарядов с ячейки на ячейку. В результате этого на выходе ПЗС образуется последовательность электрических дискретных сигналов, амплитуда которых соответствует величине заряда на ячейках мишени ПЗС.

Максимум чувствительности ПЗС находится в ближней ИК-области, что позволяет их эффективно применять в ИК-диапазоне.

Электрический сигнал на выходе вакуумной передающей трубки или ПЗС усиливается и передается по проводам или в виде радиосигналов распространяется в атмосфере к телевизионному приемнику. Последний выполняет обратные функции, преобразуя электрический сигнал в изображение, яркость каждого элемента которого эквивалентна амплитуде соответствующего сигнала. Формирование изображения производится на экране приемной вакуумной трубки или экрана на жидких кристаллах.

В вакуумной приемной телевизионной трубке (кинескопе) изображение создается на ее экране электронным лучом, модулируемым электрическим сигналом и перемещающимся с помощью магнитного поля катушек отклонения по горизонтали (строке) и вертикали (по кадру) синхронно с лучом передающей трубки. Синхронность обеспечивается путем передачи синхронизирующих сигналов в виде групп импульсов, моменты времени формирования которых соответствуют границам строк и кадров. Синхроимпульсы совместно с сигналом изображения образуют полный телевизионный сигнал. При приеме из телевизионного сигнала выделяются синхроимпульсы, которые синхронизируют работу устройств кадровой и строчной развертки. Эти устройства формируют сигналы, при прохождении которых по катушкам отклонения создается растр изображения.

Основными характеристиками телевизионных средств наблюдения являются чувствительность передающих трубок (ПЗС) и разрешающая способность. Чувствительность определяется чувствительностью материала фотокатода, а разрешение - количеством строк разложения изображения.

Современные передающие телевизионные трубки имеют чувствительность, обеспечивающую телевизионное наблюдение в сумерках.

Разрешение современных телевизионных систем наблюдения стандартизировано и составляет 625 строк. Чем выше разрешение, тем меньше длительность сигнала элемента изображения и тем шире спектр телевизионного сигнала. Минимальный спектр телевизионного сигнала, передаваемого с частотой кадра 25 Гц и разрешением в 625 строк, составляет 6.5 МГц, полного телевизионного сигнала (со звуковым сопровождением) - 8 МГц. Для передачи таких сигналов на значительные расстояния

(сотни км) необходима большая мощность передатчика.

Проблемы, возникающие из-за широкой полосы телевизионного сигнала, существует при его записи на магнитную ленту. В аудимагнитофоне максимальная частота сигнала достигает 20 кГц, что составляет менее 1/300 части верхней частоты видеосигнала. Поэтому для записи видеосигнала на принципах аудиозаписи необходимо увеличить скорость перемещения ленты в 300 раз, что неприемлемо. В видеомагнитофоне реализован комплекс мер, обеспечивающих качество изображения, близкое к телевизионному, при приемлемых потребительских показателях видеомагнитофона и видеокассеты (габаритах, весе, времени записи на кассете). С этой целью при видеозаписи уменьшают полосу частот до 4-6 МГц, а для уменьшения линейной скорости перемещения магнитной ленты производится поперечно-строчная (поперек ленты) и наклонно-строчная (под острым углом к направлению движению ленты) запись видосигналов на магнитную ленту с помошью вращающихся одной или нескольких (до 4-х) головок. Сигналы звукового сопровождения и управления записываются на боковых краях магнитной ленты. Такие методы записи видеосигналов позволяют при сохранении высокой скорости движения ленты относительно головки значительно (порядка 100 раз) уменьшить продольную ее скорость и обеспечить приемлемое время записи на одной кассете. Для уменьшения влияния паразитной амплитудной модуляции из-за переменного контакта головки с лентой применяют частотную модуляцию с переменным индексом модуляции для разных частот и записывают на ленту частотно-модулированный сигнал. Кроме того, сохранение требуемых временных соотношений достигается применением высокоточных лентопротяжных механизмов, систем автоматического регулирования электродвигателями и цифровых корректоров временных искажений.

Видеомагнитофоны с поперечно-строчной записью обеспечивают высокое качество изображения и звукового сопровождения, но громоздки и сложны в эксплуатации. Конструктивно более простыми являются профессиональные и бытовые видеомагнитофоны с наклонно-строчной записью.

В зависимости от требований к качеству записи и соответствующей скорости “лента-головка” применяют ленты шириной 50.8, 25.4, 19, 12.65 и менее. Широкая лента используется в профессиональных видеомагнитофонах, 12.65 мм и менее - в бытовых. Разнообразие значений ширины ленты в сочетании с разными способами записи обусловили множество форматов записи: для ленты шириной 50.6 мм - Q, 25.4 мм - B, C , 19.05 мм - U, 12.65мм - L, M11, VHS, Beta и др. В бытовой видеозаписи наибольшее распространение получили форматы VHS и Beta. Видеофонограммы формата VHS для отечественной бытовой аппаратуры имеют следующие параметры:

- скорость головки относительно ленты - 4.85 м/с;
- продольная скорость ленты - 23.39 мм/с;
- ширина видеострочки - 0.04 мм;
- ширина дорожки звука - 0.3 мм;
- ширина дорожки управления - 0.75 мм;
- угол наклона строчки относительно края ленты - около 6 град.

Малая продольная скорость ленты позволяет на стандартной кассете с размерами 188x104x25 мм производить непрырывную запись изображения в течение 3-5 часов (в зависимости от толщины ленты и других мер.

В целях повышения качества изображения развивается цифровая видеозапись в форматах D1-D5, а в интересах сокращения габаритов и веса, что важно для решения задач по добыванию информации, - переход на малогабаритные кассеты. На базе широко применяемого формата VHS предложены форматы VHS-C для кассеты с габаритами 92x59x22.5 мм), Video 8 (95x62.5x15 мм, ширина ленты 8 мм) и малогабаритная кассета МК (102x63x12) с шириной ленты 3.8 мм. В современных видеомагнитофонах удается также снизить скорость до 1 см/с и менее с соответствующим увеличением времени записи. Например, в цифровом видеомагнитофоне EV-A80 (Sony) достигнута скорость

ленты 0.6/0.3 см/с, время записи в формате V-8 - 540/1120 мин. с разрешением 250 строк.

При существующих стандартах на параметры телевизионных средств наблюдения их разрешение на порядок хуже разрешения фотоснимков. Для повышения четкости изображения разрабатываются средства с повышенными в 2 раза разрешением и частотой кадров. Но при этом соответственно увеличивается ширина спектра телевизионного сигнала со всеми вытекающими из этого недостатками. Поэтому для широкого внедрения качественного телевидения необходимо решить проблему сокращения ширины спектра его телевизионного сигнала.

Для телевизионного наблюдения в ИК-диапазоне применяют телевизионные приборы с ЭОП, устанавливаемые перед вакуумными передающими трубками и ПЗС.

Для наблюдения в оптическом диапазоне применяют также лазеры, лучи которых в видимом или ИК-диапазонах подсвечивают объекты в условиях низкой освещенности. Для этой цели луч лазера с помощью качающихся зеркал сканирует пространство с наблюдаемыми объектами, а отраженные от них сигналы принимаются фотоприемником так же как при естественном освещении.

С целью обеспечения скрытого наблюдения средства наблюдения камуфлируются под бытовые приборы и личные вещи. Некоторые средства приведены в табл. 3.5.

Таблица 3.5.

Наименование	Тип, фирма	Характеристики
Поясная видеокамера	PK5110, ELECTRONIC	ПЗС, 280x350 линий, мин. освещение 3 лк, угол зрения 55, 180 г, передатчик PK 1910,170 г
Поясная видеокамера с магнитофоном	PK6020, ELECTRONIC	ПЗС, 280x350, 3 лк, 180 г, магнитофон 50x110x170 мм, время записи 3 ч.
Цветная видеосистема в кейсе	PK5325, ELECTRONIC	Включает камеру “Сатикон”, видеомагнитофон, устройство питания, монитор, 460x330x120 мм, 13.2 кг
Видеокамера-зажим	OSV-4, KNOWLEDGE EXPRESS	Видеокамера в булавке для галстука, 2 лк, соединена с видеомагнитофоном в кармане, продолжительность работы видеомагнитофона 3ч. .
Автомобильная видеокамера	PK1780-s, ELECTRONIC	Объектив в автомобильной антенне, видеокамера с передатчиком, дальность 3 км, 83x167x49 мм, 460 г
Видеокамера в датчике пожара	OVS-12, KNOWLEDGE EXPRESS	2 мм объектив с f=13.3 мм, ручное и автоматическое панорамирование - 30-260 град.
Видеокамера в картине	OVS-13, KNOWLEDGE EXPRESS	Камера аналогична OVS-12, картина размером 12.5x17.8 см
Фотокамера- часы	PK420, ELECTRONIC	Диаметр 34 мм, толщина 10 мм, вес 70 г, 7 снимков диаметром 5.5 мм
Фотокамера в дипломате	PK1690,- S, ELECTRONIC	Стандартный размер портфеля-дипломата, 7.5 кг, пленка 35 мм, съемка автоматизирована

Примечание. ПЗС - приборы с зарядовой связью.

Приборы ночного видения

Для визуально-оптического наблюдения в инфракрасном диапазоне необходимо невидимое для глаз изображение в инфракрасном диапазоне (более 0.76 мкм) переместить в видимый диапазон. Для визуально-оптического наблюдения в ИК-диапазоне применяются приборы ночного видения (ПНВ).

Основу приборов ночного видения составляет электронно-оптический преобразователь (ЭОП), преобразующий невидимый глазом свет в видимый. Самый

простой ЭОП, так называемый стакан Холста, состоит из двух параллельных пластин, помещенных в стеклянный стакан, из которого выкачан воздух (рис. 3.2).

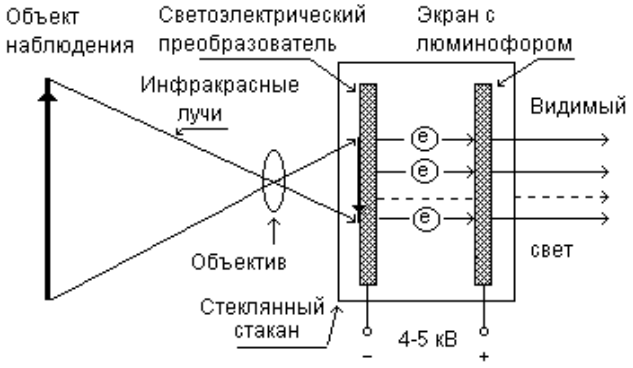


Рис. 3.2. Схема стакана Холста.

Внешняя сторона первой пластины - фотокатода покрыта светочувствительным материалом (слоем из окиси серебра с цезием), второй представляет металлизированный экран с люминофором. Между пластинами создается сильное электрическое поле величиной 4-5 кВ.

На фотокатод объективом проецируется изображение в ИК-диапазоне. В каждой точке фотокатода под действием фотонов света возникают свободные электроны, количество которых пропорционально яркости соответствующей точки изображения. Электрическое поле между пластинами вырывает свободные электроны из фотокатода и, разгоняя, устремляет их к экрану с люминофором. В моменты столкновения электронов с люминофором возникают вспышки света, яркость которых пропорциональна количеству электронов. Таким образом, на экране с люминофором формируется изображение в видимом диапазоне, повторяющее исходное в ИК-диапазоне.

Однако параметры (чувствительность, разрешение) рассмотренного ЭОП невысокие и не обеспечивают наблюдение при низкой освещенности и, следовательно, добывание демаскирующих признаков об объекте с мелкими деталями. С момента создания первого ЭОП в виде стакана Холста разработано несколько поколений этих приборов (от нулевого до 3-го). ЭОП 2 и 3-го поколений, которые используются в настоящее время, имеют чувствительный фотокатод, а между пластинами камеры размещается так называемая микроканальная пластина. Пластина содержит приблизительно 5000 микроканалов на 1 мм (диаметр канала достигает 12 мкм), внутри которых движутся электроны фотокатода. В результате устранения взаимного влияния электронов от соседних точек фотокатода, движущихся по разным микроканалам, достигается повышение разрешающей способности прибора ночного видения с микроканальной пластиной. Кроме того, в процессе движения электронов внутри каналов происходит “размножение” электронов в результате выбивания их из стенки канала при столкновении с нею движущихся электронов.

Основные показатели приборов ночного видения различных поколений приведены в табл. 3.1.

Таблица 3.1.

Поколения	Коэффициент усиления	Разрешающая способность, лин/мм	Чувствительность, мкА/лм
I поколение: - однокамерные - двухкамерные - трехкамерные	 80 4000 50000	 65 40 25	 * * *
II поколение	7000-15000	28	270
III поколение	20000-35000	35	1250

На основе ЭОП 2 и 3-го поколений созданы различные приборы ночного видения,

включающие ночные бинокли и очки, артиллерийские приборы и прицелы для различных образцов военной техники. Самые малые по размерам ПНВ - очки на базе ЭОП 3-го поколения имеют угол зрения 40 град., дальность наблюдения (обнаружения) 500м при естественном освещении около 10^{-3} лк, массу 700 г.

Приборы ночного видения эффективно работают в условиях естественного ночного освещения, но не позволяют проводить наблюдения в полной темноте (при отсутствии внешнего источника света). Их чувствительности недостаточно для приема световых лучей в ИК-диапазоне, излучаемых телами.

Приборы ночного видения (ПНВ) разделяют на 3 группы:

- приборы малой дальности действия (ночные очки), позволяющие видеть фигуру человека на расстоянии 100-200 м. Вес и габариты этих приборов позволяют носить их в карманах, сумках, портфелях;
- приборы (ночные бинокли, трубы) средней дальности (человек виден до 300-400 м), наблюдение ведется с помощью с рук;
- приборы большой дальности действия (до 1000 м), устанавливаемые для наблюдения на треноге или подвижном носителе.

Например, прибор ночного видения - бинокль фирмы Noctron (США) имеет фокусное расстояние 135 мм, угол поля зрения - 10.6^0, масса 1.98 кг, габариты 320x80x210 мм, дальность наблюдения человеком 300-400 м.

По способу подсветки приборы ночного видения условно разделяют на три типа:
- объект наблюдения подсвечивается с помощью искусственного источника ИК-излучения, размещенного на приборе ночного видения;
- с подсветкой от естественного освещения;
- принимающего собственное тепловое излучение объекта наблюдения.

Приборы ночного видения первого типа содержит ИК-фару в виде обычного источника света мощностью 25-100 Вт, закрытой спереди специальным фильтром. Например, прибор ночного видения с подсветкой «Аргус» позволяет вести наблюдение в полной темноте объектов на удалении до 120 м [14]. На этом удалении можно различить силуэт человека и определить тип транспортного средства. Опознать человека по признакам внешности и лица можно на значительно меньшем расстоянии 35-50 м. Приборы ночного видения без подсветки при освещенности ночью в летнее время (приблизительно 0.005 лк) позволяют видеть фигуру человека на расстоянии до 300-400 м. ПНВ без подсветки отечественного производства «Ворон» имеет пороговый уровень освещенности для визуального обнаружения объектов 0.001 лк, для регистрации - 0.01 лк. Его разрешающая способность не менее 28 лин/мм, диапазон автоматической регулировки 100000, напряжение питания 5-9 В, масса - не более 1.2 кг. Приборы третьего типа называются тепловизоры.

Тепловизоры

Преграду для создания прибора наблюдения в полной темноте на рассмотренных принципах создают тепловые шумы фотокатодов. Снижение уровня этих шумов достигается снижением температуры фотоприемника. Для достоверного выделения энергии теплового излучения на фоне собственных шумов фотоприемника последний нуждается в охлаждении до весьма низких температур в интервале -70^o - $(-200)^o$ С.

Способы охлаждения фотоприемника реализуются в тепловизорах, типовая схема которого приведена на рис. 3.3.

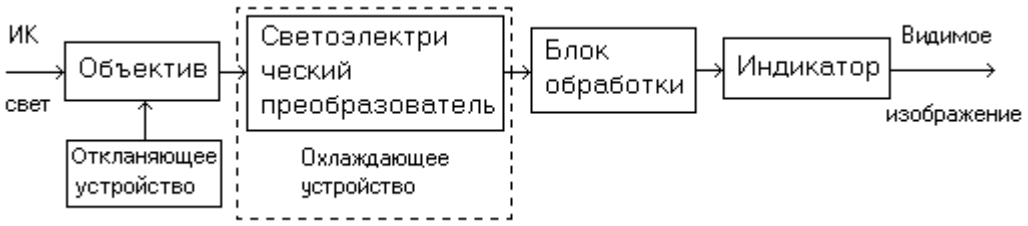


Рис. 3.3. Схема тепловизора.

В качестве электронно-оптических преобразователей современных тепловизоров используются линейки с фотодиодами (60-200 штук), образующими строку кадра. Развертка по вертикали (сканирование) производится путем механического качания зеркала, направляющего световые лучи от объектива к фотоприемнику. Охлаждение фотоприемников осуществляется специальными микрогабаритными холодильниками, в которых реализуются принципы термоэлектрического охлаждения, расширения газа в вакууме, термодинамические циклы Стирлинга и др. Например, ручной французский тепловизор IRGO, работающий в диапазоне 3-5 мкм, обеспечивает наблюдение в полной темноте на расстоянии до 1 км с четкостью 200x120 элементов разложения изображения и с частотой сканирования 25 Гц. Изображение в видимом диапазоне формируется на экране с матрицей из светодиодов, излучающих желтый цвет. Мощность энергопотребления прибора составляет 10 Вт, масса с батареей питания - 4 кг.

Основными характеристиками технических средств наблюдения в ИК-диапазоне, влияющие на их возможности, являются следующие:

- спектральный диапазон;
- пороговая чувствительность по температуре;
- фокусное расстояние объектива;
- диаметр входного отверстия объектива;
- угол поля зрения прибора;
- коэффициент преобразования (усиления) ЭОП;
- интегральная чувствительность фотокатода ЭОП.

3.1.2. Способы и средства наблюдения в радиодиапазоне

Радиолокационное и радиотепловое наблюдение осуществляется в радиодиапазоне электромагнитных волн с помощью способов и средств радиолокации и радиотепловидения.

Для получения радиолокационного изображения в радиолокаторе формируется зондирующий узкий сканирующий (перемещающейся по определенному закону по горизонтали и вертикали) луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который перемещаясь синхронно с зондирующим лучем «рисует» на экране изображение объекта. Принципы радиолокационного наблюдения показаны на рис.3. 6.

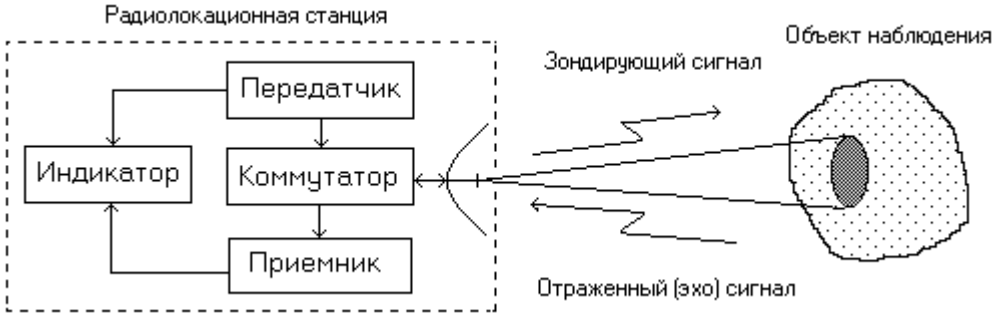


Рис. 3.6. Принципы радиолокационного наблюдения.

Радиолокационное изображение существенно отличается от изображения в оптическом диапазоне. Различие обусловлено разными свойствами отражающей поверхности объектов в оптическом и радиодиапазонах.

Отраженная энергия в радиодиапазоне пропорциональна площади поверхности и конфигурации объекта, электрической проводимости поверхности. Отражательная способность объекта или его элементов характеризуется эффективной площадью рассеяния.

Эффективная площадь рассеяния равна площади идеальной плоской поверхности, перпендикулярной к направлению облучения и помещенной в точке нахождения объекта, которая создает у приемной антенны радиолокатора такую же плотность потока мощности, как реальный объект.

Основными показателями радиолокационных средств наблюдения являются следующие:

- дальность наблюдения;
- разрешающая способность на местности.

Дальность радиолокационного наблюдения зависит от излучаемой радиолокатором энергии (мощности передатчика локатора) и характеристик среды распространения электромагнитной волны. Ослабление электромагнитной волны при ее распространении определяется длиной волны и степенью ослабления ее в атмосфере. Чем короче длина волны, тем прямолинейнее ее путь распространения и тем больше она затухает в атмосфере. Но одновременно тем выше может быть обеспечена разрешающая способность радиолокатора на местности.

Разрешение радиолокатора на местности определяется величиной пятна, которое создает луч радиолокационной станции при облучении поверхности объекта или местности. Пятно тем меньше, чем уже диаграмма направленности антенны радиолокатора. Последняя, в свою очередь, определяется соотношением геометрических размеров конструкции антенны и длины волны. Кроме того, следует иметь ввиду, что электромагнитная волна отражается от объекта или его деталей, если их размеры, по крайней мере, соизмеримы с длиной волны. Если размеры их значительно меньше, то волна эти объекты огибает. В связи с этими с этими соображениями наиболее широко в радиолокации применяется сантиметровый диапазон с тенденцией перехода в мм-диапазон.

По дальности действия наземные радиолокаторы различаются на малой, средней, большой дальности и сверхдальнего действия. РЛС малой дальности применяют для обнаружения людей и транспортных средств на расстоянии в сотни метров, средней - единицы км, большой - десятки км. Точность определения координат наземных РЛС составляет по дальности 10-20% и около градуса по азимуту.

Сверхдальные РЛС используют эффект, открытый в 60-е годы Н. И. Кабановым. Этот эффект состоит в способности радиоволн в декаметровом диапазоне распространяться на большие расстояния не только в прямом, но и обратном направлениях. Отражаясь от объектов на земной поверхности на удалении 800-4000 и более км от РЛС, электромагнитные волны, несущие информацию об их демаскирующих признаках, принимаются и регистрируются приемником радиолокатора. Однако из-за нестабильности ионосферы разрешение таких РЛС значительно хуже, чем у надгоризонтных радиолокаторов.

Повышение разрешающей способности радиолокаторов без значительного увеличения размеров антенны, что особенно важно для воздушного и космического радиолокационного наблюдения, обеспечивается в радиолокационных станциях бокового обзора (РЛС БО). Они размещаются на самолетах и разведывательных КА.

В РЛС БО применяются два вида антенн: вдольфюзеляжные и с синтезированной (искусственной) апертурой антенны (РСА).

Принцип работы радиолокатора бокового обзора иллюстрируется на рис. 3.7.

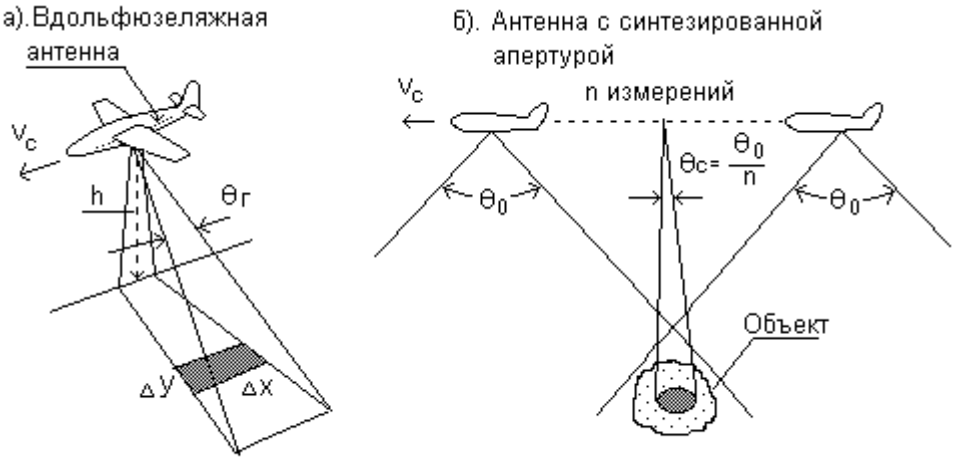


Рис.3.7. Принцип работы радиолокатора бокового обзора.

Элементы антенны первого вида размещают вдоль фюзеляжа самолета с обеих его сторон или в подвесном контейнере-обтекателе. Благодаря этому размер антенны можно увеличить до 15 м. Такая антенна создает в боковом направлении узкую (доли градусов) диаграмму направленности в горизонтальной плоскости и широкую - в вертикальной. В текущий момент времени она облучает на земной поверхности площадку шириной Δx и длиной Δy (см. рис.3.7). Так как зондирующий сигнал проходит до элементов этой площадки и после отражения к антенне разные пути, то лучи в точке приема имеют разные фазы. На приемной стороне сигналы, отраженные от разных участков площадки, упорядочиваются по фазе, в результате чего обеспечивается возможность увеличить разрешение в вертикальной плоскости до значения, соответствующего шагу дискретизации фазы. Величина же шага ограничивается точностью определения точности фазы и возможностями бортового компьютера.

Просмотр земной поверхности по направлению полета самолета или космического аппарата производится за счет движения носителей РЛС

БО с разрешением на местности, соответствующему ширине диаграммы направленности антенны в горизонтальной плоскости - по азимуту.

Повышение угловой разрешающей способности РЛС с синтезированной апертурой антенны основано на формировании узкой диаграммы направленности по азимуту с помощью искусственно создаваемой антенной решетки. Диаграмма направленности антенной решетки, формируемой в результате когерентного (с учетом фазы) сложения радиоволн от n одинаковых ее элементов размером d, что и антенна размером nd.

В РЛС применяется небольшая антенна, широкая диаграмма направленности которой неподвижна относительно самолета и направлена перпендикулярно линии полета. При полете самолета антенна РЛС последовательно занимает в пространстве положения на прямой траектории полета самолета, эквивалентные положениям элементам гипотетической антенной решетки. В результате запоминания сигналов, последовательно принимаемых антенной в каждой точке траектории полета самолета, и их когерентного суммирования достигается существенное повышение разрешающей способности на местности. Размер решетки (синтезированной апертуры) соответствует длине участка траектории, на котором производится запоминание и когерентное суммирование сигналов. Используя этот метод, можно увеличить разрешающую способность РЛС по азимуту в 100 и более раз.

3.2. Способы и средства перехвата сигналов

Перехват носителей в виде электромагнитного, магнитного и электрического полей,

а также электрических сигналов с информацией осуществляют органы добывания радио и радиотехнической разведки. При перехвате решаются следующие основные задачи:

- поиск по демаскирующим признакам сигналов с информацией в диапазоне частот, в которых они могут;
- обнаружение и выделение сигналов, интересующих органы добывания;
- прием (селекция, усиление) сигналов и съем с них информации;
- анализ технических характеристик принимаемых сигналов;
- определение местонахождения (координат) источников представляющих интерес сигналов;
- обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

Упрощенная структура типового комплекса средств приведена на рис. 3.8.

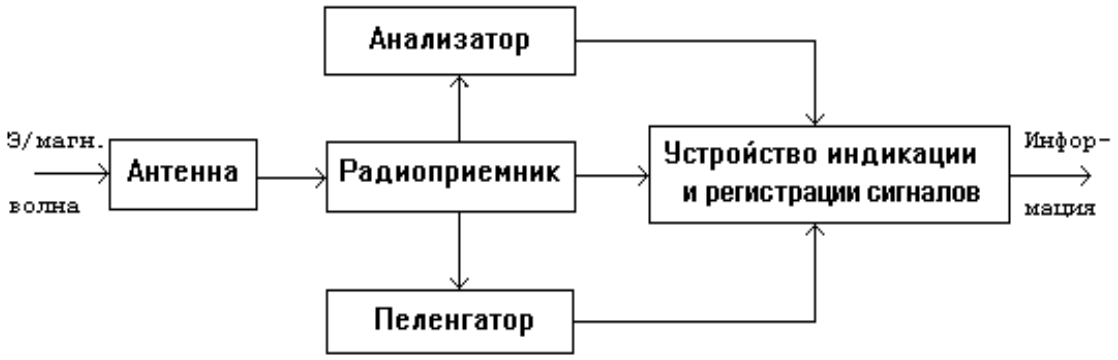


Рис. 3.8. Структура комплекса средств перехвата.

Типовой комплекс включает:

- приемные антенны;
- радиоприемник;
- анализатор технических характеристик сигналов;
- радиопеленгатор;
- устройство обработки сигналов;
- устройство индикации и регистрации.

Антенна предназначена для преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствует аналогичным характеристикам электромагнитной волны.

В радиоприемнике производится селекция сигналов по частоте, усиление и детектирование (демодуляция) выделенных радиосигналов с целью получения сигнала на носителе в виде электрических первичных сигналов: речевых, цифровых данных, видеосигналов.

Для анализа радиосигналов после селекции и усиления они подаются на входы комплекса измерительной аппаратуры, осуществляющей автоматическое или автоматизированное измерение их параметров: частотных, временных, энергетических, вида модуляции, видов и структуры кодов и др. Эти комплексы различаются по диапазонам частот, функциям, принципам построения (аналоговые, цифровые).

Радиопеленгатор определяет направление на источник излучения (пеленг) или его координаты.

Устройство обработки и регистрации производит первичную обработку информацию (сведений и данных) и регистрирует ее для последующей обработки.

Каждое из этих средств характеризуется набором определенных функций и параметров.

Антенны

Антенны преобразуют энергию электромагнитной волны в электрические сигналы и представляют конструкцию из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования. Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация основных из которых представлена на рис. 3.9.

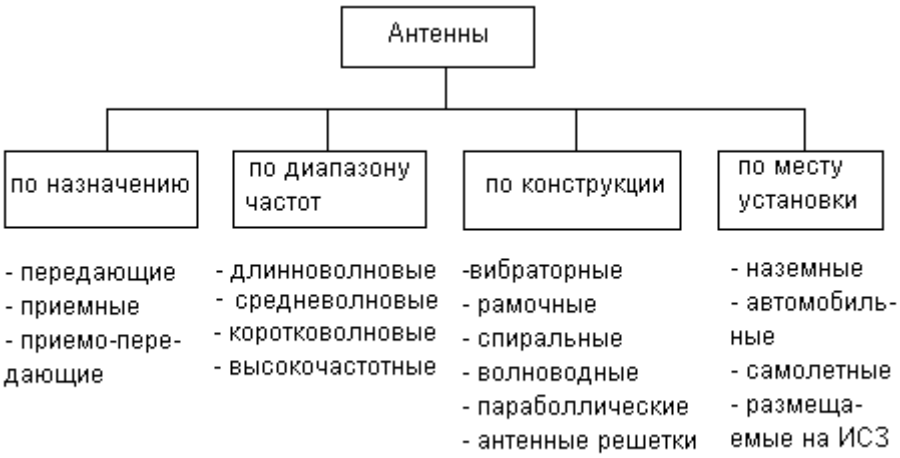


Рис. 3.9. Классификация антенн.

Назначение передающих и приемных антенны ясно из их наименований. По своим основным электрическим параметрам они не отличаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящиеся под высоким напряжением.

Эффективность антенн зависит от согласования размеров элементов антенны с длинами излучаемых или принимаемых волн. Длина согласованной с длиной волны электромагнитного колебания штыревой антенны близка к $\lambda/4$, где λ - длина рабочей волны. Поэтому размеры и конструкция антенн отличаются как для различных диапазонов частот, так и внутри диапазонов.

Если для стационарных антенн требование к геометрическим размерам антенны может быть достаточно просто выполнено для коротких и ультракоротких волн, то для антенн, устанавливаемых на мобильных средствах, оно неприемлемо. Например, рациональная длина антенны для обеспечения связи на частоте 30 МГц составляет 2.5 м, что неудобно для пользователя. Поэтому применяют укороченные антенны, но при этом уменьшается их КПД. По данным укорочение антенны в 2 раза уменьшает КПД до 60%, в 5 раз (до 50 см) - до 10%, а КПД антенны, укороченной в 10 раз, составляет всего около 3% от рационального варианта.

По конструкции антенны разделяются на проволочные (вибраторные), рупорные, параболические, рамочные, спиральные, антенные решетки и различные их комбинации.

Возможности антенн как приемных, так и передающих определяются следующими характеристиками:

- диаграммой направленности;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

Диаграмма направленности представляет графическое изображение уровня

принимаемого сигнала от угла поворота антенны в горизонтальной и вертикальной плоскостях. Диаграммы изображаются в прямоугольных и полярных координатах (см. рис. 3.10).

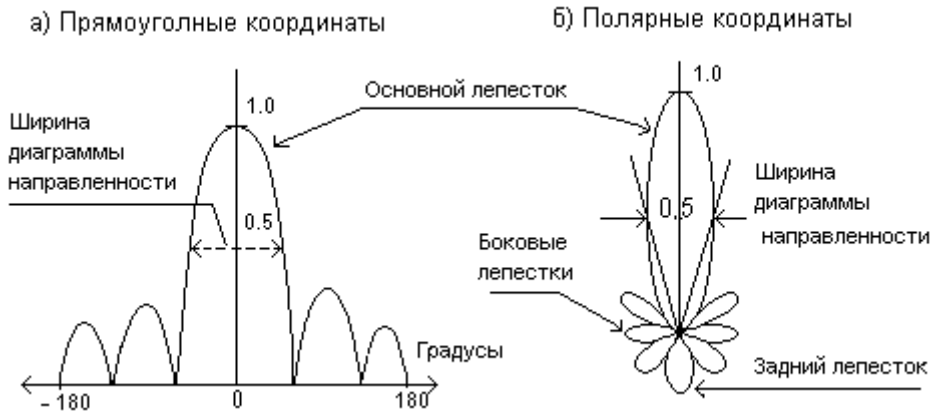


Рис. 3.10. Диаграмма направленности антенн.

Они могут иметь разнообразный и изрезанный характер, определяемый механической конструкцией и электрическими параметрами. Лепесток диаграммы направленности с максимумом мощности излучаемого или принимаемого электромагнитного поля называется главным или основным лепестком, остальные боковыми и задними. Соотношение между величинами мощности основного лепестка по сравнению с остальными характеризует направленные свойства антенны. Ширина главного лепестка диаграммы измеряется углом между прямыми, проложенными из начала полярных координат до значений диаграммы, соответствующих половине максимальной мощности излучения или 0.7 напряжения электрического сигналов приемной антенны. Чем уже ширина диаграммы направленности антенны, тем выше ее коэффициент направленного действия.

Коэффициент направленного действия (КНД) определяет величину энергетического выигрыша, который обеспечивает направленная антенна по сравнению с ненаправленной. Потери электрической энергии в антенне оцениваются коэффициентом полезного действия (КПД), равного отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь.

Произведение этих двух коэффициентов определяет коэффициент усиления антенны (КУ). Так как КНД >1, а КПД <1, то коэффициент усиления в зависимости от значений сомножителей может теоретически принимать значения как меньше, так и больше 1. Чем выше КУ, тем больший энергетический эффект обеспечивает антенна, но тем точнее необходимо ориентировать направление основного лепестка на источник излучения. Для параболической антенны коэффициент усиления антенны рассчитывается по формуле

$$КУ=4\pi S_{эф}/\lambda^2,$$

где $S_{эф}$ - эффективная площадь зеркала антенны;

λ - длина электромагнитной волны.

Для линейных антенн (например, вибраторов) КУ характеризуется действующей высотой или длиной $h_a=E_a/E$, где E_a - максимальное значение наводимой в антенне электродвижущей силы, E - напряженность электромагнитного поля в точке приема. Полоса частот, в пределах которых сохраняются заданные технические характеристики антенны, называется полосой ее пропускания.

Создание антенн с высоким коэффициентом усиления и широкой полосой пропускания представляет основную проблему в области конструирования антенн. Чем выше КУ, тем труднее обеспечить широкополосность антенны. В зависимости от полосы пропускания антенны разделяются на узкополосные, широкополосные, диапазонные и широкодиапазонные.

Узкополосные антенны обеспечивают прием сигналов в диапазоне 10% от основной

частоты. У широкополосных антенн эта величина увеличивается до (10-50)%, диапазонные антенны имеют коэффициент перекрытия (отношение верхней частоты полосы пропускания антенны к нижней) составляет 1.5-4, а у широкополосных антенн это отношение достигает значений в интервале 4-20.

Совокупность однотипных антенн, расположенных определенным образом в пространстве, образуют антенную решетку. Сигнал антенной решетки соответствует сумме сигналов от отдельных антенн. Различают линейные (одномерные) и плоские (двухмерные) антенные решетки. Антенные решетки, у которых можно регулировать фазы сигналов отдельных антенн, называют фазированными антенными решетками. Путем изменения фаз суммируемых сигналов можно менять диаграмму направленности в горизонтальной и вертикальной плоскостях и производить быстрый поиск сигнала по пространству и ориентацию антенны на источник излучения.

Радиоприемник

Радиоприемник - основное техническое средство перехвата, осуществляющего поиск, селекцию, прием и обработку радиосигналов. В состав его входят устройства, выполняющие:

- перестройку частоты настройки приемника и селекцию (выделение) нужных радиосигналов;
- усиление выделенных сигналов;
- детектирование (съем информации);
- усиление видео или низкочастотного первичного сигнала.

Различают два вида радиоприемников: прямого усиления и супергетеродинные. Появившиеся первыми приемники прямого усиления уступили супергетеродинным почти во всех радиодиапазонах, за исключением сверхвысоких частот. Такая тенденция объясняется более высокой селективностью и чувствительностью супергетеродинного радиоприемника по сравнению с приемником прямого усиления.

В приемниках прямого усиления, как следует из названия, сигнал на входе приемника (выходе антенны) селектируется и усиливается без изменения его частот. Качество информации, снимаемой с этого сигнала, тем выше, чем меньше уровень помех (сигналов различной природы с частотами, близкими частоте настройки приемника). В идеале цепи селекции должны обеспечивать П - образную форму с полосой пропускания, равной ширине спектра селектируемого сигнала.

Такие фильтры имеют многозвенную, достаточно сложную конструкцию из тщательно настраиваемых LC - элементов или реализуются с использованием поверхностных акустических волн.

Сложность проблемы обеспечения избирательности в радиоприемниках прямого усиления обусловлена техническими трудностями создания одновременно перестраиваемых по частоте узкополосных фильтров с высокими показателями по селективности, в особенности при их промышленном производстве. Только на сверхвысоких частотах удалось достигнуть высоких показателей по чувствительности и избирательности благодаря применению в широкополосных цепях высокой частоты специальных материалов и устройств: фильтров из железоиттриевого граната и малошумящих ламп бегущей волны.

В супергетеродинном приемнике проблема одновременного обеспечения высоких значений чувствительности и селективности решена путем преобразования принимаемого высокочастотного сигнала после его предварительной селекции и усиления в усилителе высокой частоты в сигнал постоянной частоты, называемой промежуточной частотой (см. рис. 3.11).

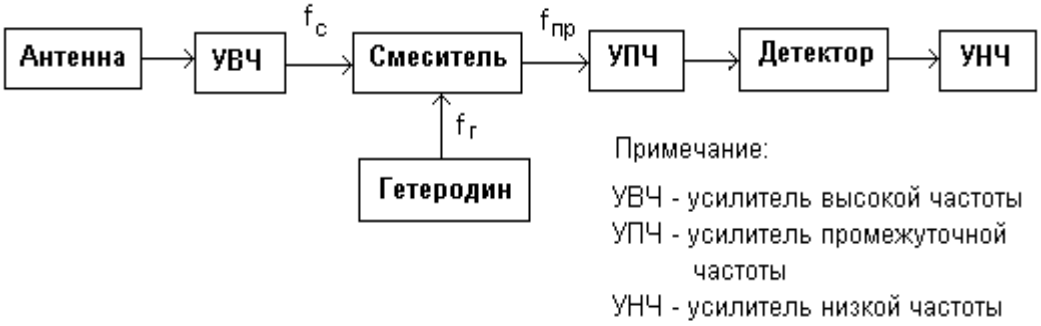


Рис. 3.11. Структура супергетеродинного приемника.

После преобразования усиление и селекция выполняются применительно к сигналам промежуточной частоты. Для постоянной промежуточной частоты задачи по обеспечению высокой избирательности и чувствительности решаются проще и лучше. Преобразователь частоты состоит их гетеродина и смесителя. Гетеродин представляет собой перестраиваемый вручную или автоматически высокочастотный генератор гармонического колебания с частотой, отличающейся от частоты принимаемого сигнала на величину промежуточной частоты. Процесс преобразования частоты происходит в смесителе, основу которого составляет нелинейный элемент (полупроводниковый диод, транзистор, радиолампа). На него поступают принимаемый сигнал с частотой fc и гармонический сигнал гетеродина с частотой $f_г$. На выходе смесителя создается множество комбинаций гармоник принимаемого сигнала и колебаний гетеродина, в том числе на промежуточной частоте $f_п=f_с- f_г$. Селективные фильтры усилителя промежуточной частоты пропускают только сигналы промежуточной частоты, которые усиливаются до величины, необходимой для нормальной работы детектора. Однако супергетеродинному приемнику присущ ряд недостатков, вызванных процессом преобразования частоты. Они состоят в том, что фильтры усилителя промежуточной частоты пропускают не только полезные сигналы, частота которых равна $f_с=f_г+f_п$,, но и ложные с частотой $f_л= f_г - f_п$, симметричной (“зеркальной”) по отношению к частоте гетеродина $f_г$. Помехи на “зеркальной” частоте ослабляются путем двойного или даже тройного преобразования частот в супергетеродинном приемнике. Промежуточная частота каждого последующего преобразования понижается. В результате этого первую промежуточную частоту можно без ущерба для избирательности приемника выбрать достаточно высокой. При больших значениях промежуточной частоты “зеркальная” частота существенно отличается (на удвоенную промежуточную частоту) от сигнала и подавляется входными фильтрами радиоприемника.

Возможности радиоприемника определяются следующими техническими характеристиками:

- диапазоном принимаемых частот;
- чувствительностью;
- избирательностью;
- динамическим диапазоном;
- показателями качества принимаемой информации;
- эксплуатационными параметрами.

Диапазон принимаемых частот обеспечивается шириной полосы пропускания селективных элементов входных фильтров и фильтров усилителя высокой частоты. Настройка же приемника на нужную частоту производится путем механической или электронной перестройкой частоты гетеродина. При поиске сигналов важной характеристикой является скорость перестройки, которая в панорамных приемниках (приемниках для быстрого обзора радиодиапазонов) достигает сотни МГц за 1 мксек.

Чувствительность радиоприемника оценивается минимальной мощностью или напряжением сигнала на его входе, при которой на выходе приемника достигается отношение сигнал/помеха и мощность (напряжение), необходимые для нормальной

работы оконечной аппаратуры или восприятия информации человеком. Такая чувствительность называется реальной. Предельная чувствительность соответствует мощности (напряжения) входного сигнала, равного мощности шумов входных цепей радиоприемника. Информация полезного сигнала мощностью менее мощности шумов радиоприемника настолько сильно ими искажается, что передача информации возможна только при кодировании ее специальными помехоустойчивыми кодами.

В диапазонах дециметровых и более коротких волн чувствительность измеряют в ваттах или децибелах по отношению к уровню в 1 мВт (дБм), на метровых и более длинных - в микровольтах (мкВ). Реальная чувствительность современных профессиональных супергетеродинных приемников дециметровых и сантиметровых волн находится в пределах 10^{-12}-10^{-14} Вт, приемников метровых и более длинных волн составляет 0.1-10 мкВ.

Избирательность приемника оценивается параметрами амплитудно-частотной характеристики (АЧХ) его селективных цепей, определяющей зависимость коэффициента усиления приемного тракта от частоты. Избирательность приемника максимальная, когда его амплитудно-частотная характеристика повторяет форму спектра принимаемого сигнала. В этом случае будут приняты все его спектральные составляющие, но не пропущены спектральные составляющие других сигналов (помех). Практически реализовать это требование чрезвычайно трудно, так как спектр сигналов с различной информацией имеет изрезанную постоянно меняющуюся форму и существуют большие технически проблемы при формировании амплитудно-частотной характеристики сложной заданной формы.

Амплитудно-частотная характеристика (АЧХ) радиоприемника характеризует величину пропускания его селективных цепей в зависимости от частоты колебания сигнала. В качестве идеальной АЧХ рассматривается П-образная форма с шириной, равной средней ширине спектра сигнала.

Избирательность реального приемника оценивается двумя основными показателями: шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника, реальная форма которой имеет колоколообразный вид.

Ширина полосы пропускания определяется на уровне 0.7 по напряжению, а коэффициент прямоугольности - отношением полосы пропускания на уровне 0.1 к полосе пропускания на уровне 0.7. Чем более пологой является АЧХ радиоприемника, тем шире полоса пропускания на уровне 0.1 по отношению к уровню 0.7 и тем больше величина коэффициента прямоугольности. Коэффициент пропускания позволяет количественно оценить пологий характер амплитудно-частотной характеристики радиоприемника. Чем ближе коэффициент прямоугольности АЧХ к 1, тем круче ее скаты и тем меньше помех «пролезет» по краям полосы пропускания. С целью уменьшения мощности помех, прошедших в тракт приемника, ширину его полосы пропускания устанавливают соответствующей ширине спектра сигнала. В приемниках для приема сигналов, существенно отличающихся по ширине, например, речи и телеграфа, ширину полос пропускания различных селективных цепей изменяют путем коммутации селективных элементов (катушек индуктивности, конденсаторов).

Так как активные элементы усилительных каскадов радиоприемника (транзисторы, диоды и др.) имеют достаточно узкий интервал значений входных сигналов, при которых обеспечивается линейное усиление сигналов, то при обработке сигналов с амплитудой вне этих интервалов возникают их нелинейные искажения и, следовательно, искажение информации. В реальных условиях уровни сигналов на входе приемников, используемых для добывания информации, существенно отличаются. Например, громкость речи при приеме сигналов закладных устройств меняется в широких пределах при перемещении говорящего человека в помещении. Динамический диапазон характеризует возможности приемника по безискаженному приему сигналов различной мощности. Величина динамического диапазона оценивается отношением максимального уровня к

минимальному уровню принимаемого сигнала и измеряется в децибелах. При недостаточном динамическом диапазоне возникают искажения электрических сигналов, соответствующих громким звукам.

Для повышения динамического диапазона современные радиоприемники содержат устройство автоматической регулировки усиления (АРУ) приемного тракта в соответствии с уровнем принимаемого сигнала.

Несоответствие амплитудно-частотной и фазовой характеристик, динамического диапазона радиоприемника текущим характеристикам сигнала приводят к частотным, фазовых и нелинейным искажениям сигнала и потере информации.

Частотные искажения вызываются подавлением или изменениями составляющих спектра входного сигнала. Из-за частотных искажений сигнал на входе демодулятора приобретает форму, отличающуюся от входной.

Фазовые искажения сигнала возникают из-за нарушений фазовых соотношений между отдельными спектральными составляющими сигнала при прохождении его цепям тракта приемника.

Искажения, проявляющиеся в появлении в частотном спектре выходного сигнала дополнительных составляющих, отсутствующих во входном сигнале, называются нелинейные. Нелинейные искажения вызывают элементы радиоприемника, имеющие нелинейную зависимость между выходом и входом. Они возникают при превышении отношения значений максимальной и минимальной напряженности электромагнитной волны в месте приема динамического диапазона радиоприемника.

Эти виды искажений приводят к изменению информационных параметров сигнала на входе демодулятора и, как следствие, к искажению информации после демодуляции. Кроме указанных электрических характеристик возможности радиоприемников оцениваются также по их надежности, оперативности управления, видам электропитания и потребляемой мощности, массо-габаритным показателям.

Большие возможности по перехвату радиосигналов в широком диапазоне частот предоставляют сканирующие приемники, некоторые типы которых приведены в табл. 3.6.

Таблица 3.6.

Тип, фирма	Диапазон, МГц	Чувст., мкВ	Дин. диапазон, дБ	Полоса ПЧ, кГц	Размеры, см	Масса, кг
ESMA, R&S	20-1300	0.23	75	8/15/30/100/2000	22x15x46	20
ESMC	20-1300	0.23	75	8/15/30/100/200	22x15x46	12
AR3000A, AOR	0.15-2000	0.35	*	2.4/12/180	14x8x20	1.2
AR8000	0.5-1900	0,35	*	2.4/12/80	15x7x4	0.4
AR5000	0.01-2600	0.32	*	6.3/15/30/110/220	22x10x25	3.5
R7000A, ICOM	0.1-2000	0.5	50	2.8/6/15/150	29x11x28	8
R7100A	0.1-2000	0.35	50	2.8/6/15/150	24x9x25	6
R8500	0.1-2000	0.5	50	2.2/5.5/12/150	9x11x31	7

Примечание: чувствительность определена в режиме узкополосной ЧМ при отношении сигнал/шум на выходе детектора в полосе телефонного фильтра 12 дБ на частотах до 500 МГц.

Особенностью этих радиоприемников является возможность очень быстрой (электронной) перестройки в широком диапазоне частот. Кроме того, наиболее совершенные из сканеров содержат устройство «памяти», которое запоминает вводимые априори, а также в процессе поиска, частоты радиосигналов, не представляющие интерес для оператора. В результате такого запоминания резко сокращается время просмотра широкого диапазона частот.

Средства измерения признаков сигнала включают большой набор различных программно-аппаратных устройств и приборов, в том числе устройства панорамного обзора и анализа спектра, измерители временных параметров дискретных сигналов,

определители видов модуляции и кода.

Разрешение по наклонной дальности в РСА обеспечивается, как и в других РЛС БО, за счет импульсного режима их работы.

При наблюдении земной поверхности с помощью РСА предъявляются жесткие требования к прямолинейности траектории полета самолета, к стабильности амплитудно-фазовых характеристик приемопередающего тракта РЛС и устройств обработки сигналов, параметров среды распространения и характеристик отражения радиоволн наблюдаемых объектов. Для цифровой обработки сигналов требуется так же большая память бортового компьютера.

Наряду с тенденцией повышения частот для улучшения разрешающей способности радиолокатора в последнее время появились локаторы, использующие более низкие частоты - в пределах дециметровых и метровых волн. Главное преимущество низких частот - существенное увеличение проникающей способности облучающих сигналов. Для сухой почвы она может достигать нескольких метров. Это значит, что РЛС может наблюдать сигналы, отраженные не только от поверхности Земли или объекта, но и различными неоднородностями в глубине. Появляются дополнительные демаскирующие признаки объектов и возможность их наблюдения при маскировке, например, естественной растительностью.

3.3 Способы и средства подслушивания

Подслушивание - метод добывания информации, носителем которой является акустическая, гидроакустическая и сейсмическая волны. Этот метод добывания имеет столь же долгую историю, как и наблюдение. Во времена отсутствия специальных технических средств информация добывалась путем подслушивания речи и других звуковых сигналов ушами злоумышленника. Термин “подслушивание” сохранился и после появления разнообразных технических средств, позволяющих существенно увеличить дальность подслушивания. Некоторые из этих средств размыли границу между наблюдением и перехватом. Подслушивание, например, телефонных разговоров путем подключения приемника электрических сигналов к телефонному кабелю можно рассматривать также как перехват электрических сигналов телефонной сети.

Различают непосредственное подслушивание и подслушивание с помощью технических средств.

При непосредственном подслушивании акустические сигналы, распространяющиеся от источника звука прямолинейно в воздухе, по воздухопроводам или через различные экраны (двери, стены, окна и др.), принимаются слуховой системой злоумышленника.

Слуховая система человека обеспечивает прием акустических сигналов в диапазоне звуковых (20-20000 Гц) частот, границы которого для разных людей колеблются в широких пределах и изменяются с возрастом. Предел слышимости у молодых людей составляет 16-20 кГц, для пожилых людей он снижается в среднем до 12 кГц. Диапазон интенсивности воспринимаемых ухом звуков очень велик. На частоте 2000 Гц наиболее интенсивный звук, который человек может вынести, примерно в 10^{12} интенсивнее самого слабого воспринимаемого звука. Для представления уровня интенсивности звука при таком огромном диапазоне применяют относительную меру в дБ по отношению к порогу слышимости звука на частоте 1000 Гц. Интенсивность звука человек оценивает как его громкость. Между психологическим восприятием громкости и физической интенсивностью звука нет прямого соответствия. Громкость звука зависит не только от его интенсивности, но и от частоты. При постоянной интенсивности звуки очень высокой и очень низкой частоты кажутся более тихими, чем звуки средней частоты. Порог слышимости слуховой системы на частоте 20 Гц выше порога в диапазоне 2000-5000 Гц примерно на 70 дБ, а на частоте 10000 Гц приблизительно на 15 дБ. Следовательно, максимальная дальность непосредственного подслушивания изменяется в

широких пределах в зависимости от спектра звуков говорящего человека. Женский голос равной интенсивности слышен на большем расстоянии, чем мужской.

Уши человека плохо приспособлены для восприятия звуков, распространяющихся в твердой среде. С этой целью используются устройства - стетоскопы, которые передают колебания поверхности твердой среды распространения в слуховые проходы ушей человека. Стетоскопы широко применяются в медицинской практике для прослушивания звуков в теле человека, Они представляет собой один или два гибких звукопровода в виде резиновых или из других синтетических материалов трубок, соединенных с контактной площадкой и передающих звуковое колебание от поверхности твердого тела к ушам человека. Эти звукопроводы локализуют и направляют звуковую волну к ушам человека, а также изолируют ее от акустических помех в окружающем пространстве. Для добывания информации применяются стетоскопы, у которых площадка, контактирующая с твердой поверхностью твердой среды распространения, соединена с мембраной микрофона. Для прослушивания структурных звуков подобный акустоэлектрический преобразователь (датчика) стетоскопа прижимают или приклеивают к поверхности стены или трубы.

Основной недостаток непосредственного подслушивания - малая дальность, составляющая для речи средней (нормальной) громкости единицы и десятки метров в зависимости от уровня помех. На улице города дальность слышимости днем составляет всего несколько метров.

Подслушивание с помощью технических средств осуществляется путем:

- перехвата акустических сигналов, распространяющихся в воздухе, воде и твердых телах;
- перехвата опасных сигналов от вспомогательных технических средств и систем;
- применения лазерных систем подслушивания;
- с использованием закладных устройств;
- высокочастотного навязывания.

Конкретный метод подслушивания реализуется с использованием соответствующего технического средства. Для подслушивания применяют следующие технические средства:

- акустические приемники, в том числе направленные микрофоны;
- приемники опасных сигналов;
- акустические закладные устройства;
- лазерные системы подслушивания;
- устройства подслушивания путем высокочастотного навязывания.

Акустические приемники проводят селекцию по пространству акустических сигналов, распространяющихся в атмосфере, воде, твердых телах, преобразуют их в электрические сигналы, усиливают и селектируют по частоте электрические сигналы, преобразуют их в акустическую волну для обеспечения восприятия информации слуховой системой человека. Кроме того, электрические сигналы с выхода приемника подаются на аудимагнитофон для регистрации акустической информации.

Типовая структура акустического приемника приведена на рис. 3.12.

Рис. 3.12. Структурная схема акустического приемника.

Микрофоны

Микрофон выполняет функцию акустоэлектрического преобразования и в, основном, определяет чувствительность и диапазон частот принимаемых акустических сигналов. Конструкция микрофона определяет его диаграмму направленности.

В настоящее время созданы микрофоны, в которых используются для акустоэлектрических преобразований различные физические процессы. Классификация микрофонов приведена на рис. 3.13.

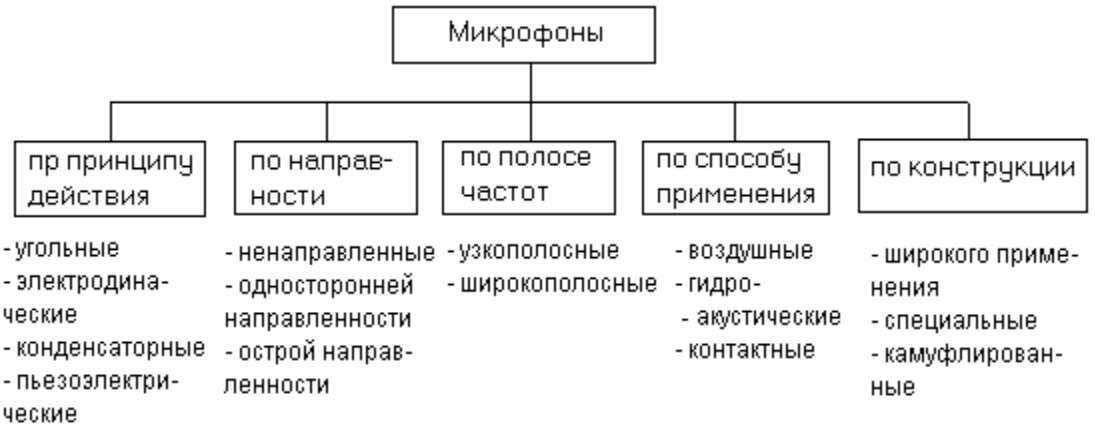


Рис. 3.13. Классификация микрофонов.

Угольные микрофоны являются наиболее древними акустоэлектрическими функциональными преобразователями. Они представляют собой круглую коробочку с гранулированным древесным углем, закрываемую тонкой металлической упругой крышкой - мембраной. К электроду, укрепленному на дне коробочки, и мембране подается напряжение около 60 В, под действием которого в массе угольного порошка протекает электрический ток. Принцип работы угольного микрофона основан на изменении сопротивления угольного порошка, находящегося между мембраной и неподвижным электродами. Акустические волны приводят мембрану микрофона в колебательное движение, под действием которой изменяется степень сжатия угольного порошка и площадь соприкосновения его гранул друг с другом. В результате этого сопротивление порошка и сила протекающего через него тока меняется в соответствии с громкостью звука, т. е. производится запись информации путем амплитудной модуляции электрического тока.

Сопротивление угольного микрофона зависит от его положения в пространстве относительно источника акустического сигнала, зернистости и технологии обработки порошка, тока питания и других факторов. Это сопротивление может составлять у низкоомных микрофонов 35-65 Ом, среднеомных - 65-145 Ом и высокоомных-145-300 Ом [17]. Угольные микрофоны имеют низкую стоимость, создают без дополнительного усилителя уровни сигналов, достаточные для передачи их на большие (десятки км) расстояния. Однако они узкополосные, имеют низкую чувствительность и нуждаются в мощном источнике тока. Используются в телефонной проводной связи.

Конструкция электродинамических микрофонов аналогична конструкции электродинамического громкоговорителя. Чувствительность их составляет 1.6-2 мВ/Па. Динамические микрофоны относительно просты, надежны в работе, могут работать в широком диапазоне температур и влажности, устойчивы к сотрясениям и широко применяются в различной звукоусилительной и звукозаписывающей аппаратуре.

В электромагнитном микрофоне в результате колебаний мембраны из ферромагнитного материала возникает эдс индукции в обмотке неподвижной катушки с сердечником, по которой протекает постоянный ток.

Конденсаторный микрофон представляет собой капсюль, состоящий из двух параллельно расположенных пластин-электродов, один из которых массивный, другой - тонкая мембрана. Электроды образуют конденсатор, емкость которого зависит от

площади пластин и расстояния между ними. К электродам подводится через резистор поляризующее постоянное напряжение. При воздействии на мембрану звуковых волн изменяются расстояния между электродами и емкость конденсатора. В результате через сопротивление протекает ток и возникает напряжение, амплитуда которых пропорциональна звуковому давлению на мембрану. При расстоянии между обкладками 20-40 мкм и поляризующем напряжении в несколько десятков вольт чувствительность микрофона достигает 10 мВ/Па. Конденсаторные микрофоны имеют высокая чувствительность, равномерную частотную характеристику в звуковом диапазоне, но стоимость их также высока. Используются в основном как измерительные микрофоны.

Разновидностью конденсаторного микрофона является электретный микрофон, мембрана которого выполнена из полимерных материалов (смол), способных в сильном электрическом поле и при высокой температуре заряжаться и сохранять электрический заряд продолжительное время. Такие материалы называют электретами. Мембрана из электрета металлизируется, между пластинами возникает разность потенциалов 45-130 В. Электретные микрофоны дешевле конденсаторных, не нуждаются во внешнем источнике и широко применяются для звукозаписывающей аппаратуры, в том числе для негласного подслушивания.

Действие пьезоэлектрического микрофона основано на возникновении эдс на поверхности пластинок из пьезоматериала, механически связанных с мембраной. Колебания мембраны под давлением акустической волны передаются пьезоэлектрической пластине, на поверхности которой возникают заряды, величина которых соответствует уровню громкости акустического сигнала.

По направленности микрофоны разделяются на ненаправленные, двухсторонней, односторонней направленности. Направленность микрофона определяется по уровню сигнала на его выходе в зависимости от поворота микрофона по отношению к источнику акустической волны в горизонтальной и вертикальной плоскостях.

Ширина диаграммы направленности микрофона оценивается в градусах на уровне 0.5 (0.7) от максимальной мощности (амплитуды) электрического сигнала на его выходе. Чем уже ширина диаграммы направленности микрофона, тем меньше доля помех попадает на его мембрану из направлений, отличающихся от направления на источник акустического сигнала с информацией. Пространственное ограничение помех повышает отношение сигнал/помеха на мембране микрофона. Частотные искажения при преобразовании акустической волны в электрический сигнал определяются неравномерностью частотной характеристики микрофона. Она определяет отклонения уровня спектральных составляющих звукового сигнала на выходе преобразователя по отношению к входному сигналу.

Для добывания информации особый интерес представляют остронаправленные микрофоны, которые позволяют существенно увеличить дальность подслушивания. Острая направленность микрофонов обеспечивается за счет соответствующей конструкции микрофона, которую можно представить в виде акустической антенны с соответствующей диаграммой направленности. Такая диаграмма направленности формируется различными акустическими антеннами, содержащими плоскую, трубчатую и параболическую поверхности.

Акустическая антенна параболического микрофона представляет собой параболическое зеркало диаметром примерно 300 мм, в фокусе которого размещается мембрана микрофона. Коэффициент усиления такого микрофона достигает 80 дБ

Трубчатый остронаправленный микрофон состоит из одной трубки диаметров около 80 мм или набора трубок, длины которых согласованы с длинами волн акустического сигнала. В торце трубок укрепляется мембраны микрофонов. Наибольшая длина трубки или их набора не превышает 650 мм. Коэффициент усиления такого микрофона достигает 90 дБ.

На основе параболической и трубчатой акустических антенн создан, например,

градиентный направленный микрофон UM 124.2, который состоит из трубки диаметром 20 мм в поролоновом ветрозащитном чехле, параболического отражателя диаметром 175 мм из акриловой пластмассы и капсюля микрофона. Длина микрофона составляет в зависимости от модификации 150 или 200 мм. Ширина диаграммы направленности такого микрофона уменьшена до 30, 20 и 10 градусов (для разных модификаций).

Поверхность плоского направленного микрофона встраивается в стенку атташе-кейса или в жилет, носимый под рубашкой и пиджаком, и передает колебания мембранам микрофонов, укрепленных на плоской поверхности. За счет увеличенной площади поверхности, воспринимающей колебания акустической волны, ширина диаграммы направленности составляет 20-25 градусов. Такой микрофон обеспечивает съем речевой информации на удалении до 50 метров от источника.

Рекламируемые возможности по дальности подслушивания направленных микрофонов (100 и более метров) завышаются. По оценке реальная дальность подслушивания речевой информации на улице города составляет при коэффициенте направленного действия микрофона 15 дБ всего 6-12 м.

По диапазону частот микрофоны разделяются на узкополосные и широкополосные. Узкополосные микрофоны предназначены для передачи речи. Широкополосные микрофоны имеют более широкую полосу частот и преобразуют колебания в звуковом и частично ультразвуковом диапазонах частот.

По способу применения микрофоны разделяются на воздушные, гидроакустические (гидрофоны) и контактные. Последние предназначены для приема структурного звука . Например, контактный стетоскопный микрофон UM 012, прикрепленный к стене помещения, позволяет прослушивать разговоры в соседнем помещении при толщине стен до 50 см. Модификацией контактных микрофонов являются ларингофоны и остеофоны, воспринимающие и преобразующие в электрические сигналы механические колебания (вибрации) связок и хрящей гортани или кости черепа говорящего. Эти приборы мало чувствительны к внешним шумам и позволяют передавать речевую информацию из помещений с высоким уровнем акустических шумов.

Возможности микрофонов определяются следующими характеристиками:

- осевой чувствительностью на частоте 1000 Гц;
- диаграммой направленности;
- диапазоном воспроизводимых частот колебаний акустической волны;
- неравномерностью частотной характеристики;
- масса-габаритными характеристиками.

Чувствительность - один из основных показателей микрофона и оценивается коэффициентом преобразования давления акустической волны в уровень электрического сигнала. Так как чувствительность микрофона для разных частот акустических колебаний различная, то она определяется на частоте наибольшей чувствительности слуховой системы человека, - 1000 Гц. Измерения проводятся для акустической волны, направление распространения которой перпендикулярно поверхности мембраны, в вольтах или милливольтах мВ на Паскаль (В/Па, мВ/Па). Чувствительность микрофона зависит в основном от параметров физических процессов в акустоэлектрических преобразователях и площади мембраны микрофона. К наиболее чувствительным микрофонам относятся электродинамические, электретные и пъезоэлектрические.

Чувствительность микрофона повышается с увеличением площади мембраны приблизительно в квадратической зависимости. Например, чувствительность конденсаторного микрофона с диаметром мембраны 6 мм, составляет 1.5-4 мВ/Па, для диаметра 12 мм-12.5 мВ/Па, а при диаметре 25 мм она увеличивается до 50 мВ/Па.

По конструктивному исполнению микрофоны бывают широкого применения, специальные миниатюрные и специальные субминиатюрные, применяемые в различных закладных устройствах.

Электрические сигналы на выходе микрофонов, используемых для добывания

информации, усиливаются в устройстве усиления и регистрации до величины, необходимой для их записи с помощью аудиомагнитофона или преобразования в акустический сигнал для обеспечения восприятия информации человеком.

Аудиомагнитофоны

Для регистрации информации широко применяются магнитофоны с вынесенными и встроенными микрофонами, в которых в единой конструкции объединяются функции микрофона и магнитофона. Последние называют диктофонами. Диктофоны для скрытного подслушивания имеют пониженные акустические шумы лентопротяжного механизма, металлический корпус для экранирования высокочастотного электромагнитного поля коллекторного двигателя, в них могут отсутствовать генераторы стирания и подмагничивания.

Характеристики некоторых типов миниатюрных магнитофонов, используемых для подслушивания, указаны в табл. 3.7.

Таблица 3.7.

Тип, фирма	Размеры, мм	Вес, г	Примечание
L400, Olympus	73x20x52	90	Запись до 3 ч
L200, Olympus	107x15x51	125	Можно носить в нагрудном кармане
PK 1985, PK Electronic	55x87x21	160	Питание 1.5 В, время работы 11 ч
Sony-909, Sony	68x65x19	*	В металлическом корпусе, 4 дорожки
AD, Knowledge Express	65x102x17	108	Запись на удалении до 15 м
TP-X900, Aiwa	167x94x43	315	Шифрование при записи

Запись производится на микрокассете со скоростью 2.4 или 1.2 см/с, длительность записи в зависимости от скорости и типа кассеты составляет от 15 мин. до 3-х часов. Различные модели диктофоны могут иметь следующие сервисные функции: активация записи голосом, возможность подключения внешнего микрофона, автостоп и автореверс, жидкокристаллический дисплей с индикацией режимов работы и расхода ленты.

Приемники опасных сигналов

Для приема опасных сигналов, несущих речевую конфиденциальную информацию, используют как бытовые, так и специальные приемники радио и электрических сигналов. Однако возможности бытовой радиоприемной аппаратуры ограничены узким диапазоном частот, выделенной для радиовещания. В диапазоне длинных волн и средних волн радиовещание осуществляется в интервале 148-1607 кГц, а в ультракоротком диапазоне в РФ - 64-74 МГц, в странах Западной Европы - 88-108 МГц.

Все более широкое распространение для подслушивания применяют сканирующие приемники, рассмотренные выше.

Для выделения, приема, усиления опасных электрических сигналов, распространяющихся по телефонным, радиотрансляционным и другим линиям, применяются селективные и специальные усилители низкой частоты. Специальные усилители содержат селективные элементы со специфическими характеристиками для выделения, например, опасных сигналов из сигналов электропитания, содержат датчики для дистанционного съема сигналов, а также имеют конструкцию, удобную для переноса и автономной работы в различных условиях скрытного подслушивания.

Закладные устройства

С целью обеспечения реальной возможностью скрытного подслушивания и существенного повышения его дальности широко применяются закладные устройства

(закладки, радиомикрофоны, “жучки”, “клопы”). Эти устройства перед подслушиванием скрытно размещаются в помещении злоумышленниками или привлеченными к этому сотрудниками организации, проникающими в помещение под различными предлогами. Такими предлогами могут быть посещения руководства или специалистов посторонними лицами с различными предложениями, участие в совещаниях, уборка и ремонт помещения, ремонт помещения и технических средств и т. д.

Закладные устройства в силу их большого разнообразия конструкций и оперативного применения создают серьезные угрозы безопасности речевой информации во время разговоров между людьми практически в любых помещениях, в том числе в салоне автомобиля.

Разнообразие закладных устройств порождает многообразие их вариантов их классификаций. Вариант классификации указан на рис. 3.14.

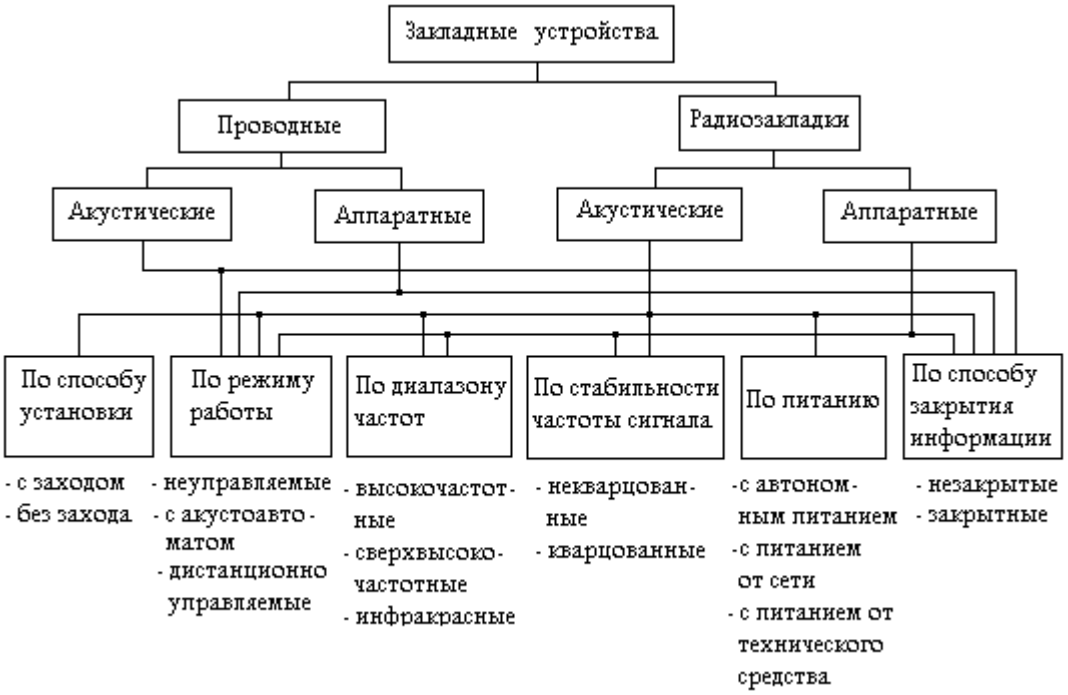


Рис. 3.14. Классификации закладных устройств.

По виду носителя информации от закладных устройств к злоумышленнику их можно разделить на проводные и радиозакладки. Носителем информации от проводных закладок является электрический ток, который распространяется по направляющим - электрическим проводам. Проводные закладки, содержащие микрофон для преобразования акустических речевых сигналов в электрические, относятся к акустическим закладным устройствам, а ретранслирующие электрические сигналы с речевой информации, передаваемые по телефонной линии, образуют группу проводных телефонных закладок.

Первые представляют собой:

- субминиатюрные микрофоны, скрытно установленные в бытовых радио- и электроприборах, в предметах мебели и интерьера и соединенные тонким проводом с микрофонным усилителем или аудиомагнитофоном, размещаемыми в других помещениях;

- миниатюрные устройства, содержащие микрофон, усилитель и формирователь сигнала, передаваемого, как правило, по телефонным линиям и цепям электропитания.

Проводные акустические закладки в виде микрофона имеют высокую чувствительность и помехоустойчивость, но наличие провода демаскирует закладки и усложняет их установку, в особенности в условиях дефицита времени. Поэтому такие закладки могут устанавливаться во время ремонта или в помещениях с возможностью достаточно простого и длительного доступа в них людей, например, в номера гостиниц.

Закладки, использующие цепи электропитания, устанавливаются в основном в местах подключения проводов электропитания к выключателям, сетевым.

Радиозакладки лишены недостатков проводных, но у них проявляется другой демаскирующий признак - радиоизлучения. В зависимости от вида первичного сигнала радиозакладки можно разделить на аппаратные и акустические. Аппаратные закладки устанавливаются в телефонных аппаратах, ПЭВМ и других радиоэлектронных средствах. Входными сигналами для них являются электрические сигналы, несущие речевую информацию (в телефонных аппаратах), или информационные последовательности, циркулирующие в ПЭВМ при обработке конфиденциальной информации. В таких закладках отсутствует необходимость в переписывании информации с акустического носителя на носитель среды распространения, что упрощает их конструкцию, и имеется возможность использования для электропитания энергию средства. Модуляция несущего колебания в них производится сигналами, циркулирующими в аппарате (в телефоне - электрическими аналоговыми сигналами, в ПЭВМ - дискретными бинарными сигналами), а для питания используется или энергия электрических сигналов или питающие напряжения аппарата, в котором установлена закладка.

Наиболее широко применяются акустические радиозакладки, позволяющие наиболее просто и скрытно устанавливать в различных местах помещения. Простейшая акустическая закладка содержит (см. рис. 3.15) следующие основные устройства: микрофон, микрофонный усилитель, генератор несущей частоты, модулятор, усилитель мощности, антенну.

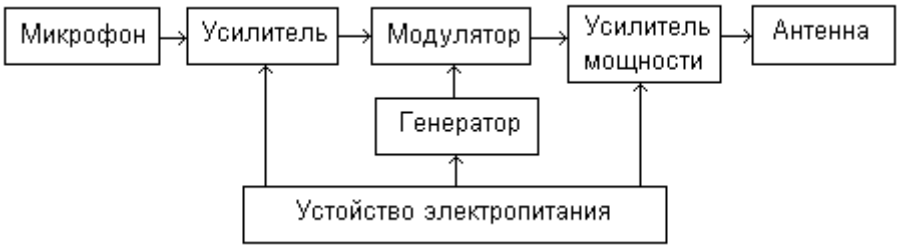


Рис. 3.15. Структурная схема акустической закладки.

Микрофон преобразует акустический сигнал с информацией в электрический сигнал, который усиливается до уровня входа модулятора. В модуляторе производится модуляция колебания несущей частоты, т. е. производится перезапись информации на высокочастотный сигнал. Для обеспечения необходимой мощности излучения модулированный сигнал усиливается в усилителе мощности. Излучение радиосигнала в виде электромагнитной волны осуществляется антенной, как правило, в виде отрезка провода.

В целях сокращения веса, габаритов и энергопотребления в радиозакладке указанные функции технически реализуются минимально-возможным количеством активных и пассивных элементов. Простейшие закладки содержат всего один транзистор.

По диапазону частот закладные устройства отличаются большим разнообразием. На ранних этапах использования закладных устройств частоты излучений их привязывали к частотам бытовых радиоприемников в УКВ-диапазоне. При массовом появлении у населения бытовых радиоприемников увеличилась опасность случайного перехвата сигналов радиозакладок посторонними лицами. Поэтому большинство типов современных закладок имеют более высокие частоты в УВЧ-диапазоне.

Для более 96% радиозакладок рабочие частоты сосредоточены в интервале 88 МГц-501 МГц, причем с частотами 92.5 МГц-169.1 МГц выпускаются 42% радиомикрофонов, а с частотами 373.4 МГц-475.5 МГц - 52% радиомикрофонов. Наиболее интенсивно используется диапазон частот 449.7 МГц-475.5 МГц, в котором сосредоточены рабочие частоты 36% образцов.

Продолжается тенденция дальнейшего повышения частот, в том числе с переходом в ГГц диапазон. С увеличением частоты передатчика уменьшается уровень помех, что позволяет снизить минимально-допустимый уровень мощности и соответственно его габариты, а также длину антенны.

В интересах повышения скрытности для радиозакладных устройств осваивается ИК-диапазон. Однако в силу большего по сравнению с радиоволнами затухания ИК-лучей в среде распространения и необходимостью прямой видимости между излучателем ИК-закладки и фотоприемником применение подобных закладных устройств ограничено.

Кроме диапазона частот на условия передачи закладкой информации влияет стабильность частоты ее передатчика. Для простых схемных решений передатчика закладки значения ее частоты изменяются в значительных пределах от температуры и питающего напряжения. Кроме того, на величину изменения (дрейфа) частоты излучения закладок, установленных вблизи рабочего места человека, например, под столешницей письменного стола, могут оказывать влияние емкость человека. Величина дрейфа рабочей частоты радиокаладок может достигать единиц мГц. В результате этого радиоприемник, настроенный на частоту радиозакладки, через некоторое время “теряет” радиосигнал. Это обстоятельство имеет важное значение для обеспечения автоматического приема сигналов радиозакладок, например, в случае, когда подслушивание производится аппаратурой в автомобиле при отсутствии в нем оператора. Поэтому частоты около половины предлагаемых на рынке радиозакладок стабилизируются. Повышение стабильности обеспечивается путем включения в колебательный контур схемы передатчика элементов, стабилизирующих его частоту. В качестве таких элементов применяются пьезоэлектрические материалы, прежде всего, кристаллы кварцы. Частота стабилизации зависит от вида среза кристалла кварца, толщины и размеров его пластины, включенной в цепь генератора. Стабилизация частоты излучения радиозакладки усложняет ее схему и увеличивает габариты передатчика, но существенно улучшает удобство работы.

Другой проблемой, возникающей при применении закладных устройств, является обеспечение их энергией в течение приемлемого для подслушивания времени. Возможности современной микроэлектроники по созданию закладных устройств в чрезвычайно малых габаритах ограничиваются в основном, массо-габаритными характеристиками автономных источников питания (химических элементов). Микрогабаритные источники тока, широко применяемые в электронных часах, обеспечивают работу закладных устройств в течение короткого времени (нескольких дней при минимально-допустимой мощности излучений для дальности до сотни метров). Для закладных устройств используются гальванические элементы с высокой удельной энергией - ртутно-цинковые, серебряные и литиевые. Усредненные характеристики этих элементов приведены в табл. 3.8.

Таблица 3.8.

Тип элемента	Рабочее напряжение, В	Максимальная емкость, Ач/кг	Плотность энергии, Втс/кг	Срок хранения, лет
Ртутный	1.2-1.25	185	120	3
Серебряный	1.5	285	130	2.5
Литиевый	3	750	350	5

Емкость гальванического элемента пропорциональна габаритам и весу. Габариты используемых в малогабаритных устройствах цилиндрических и кнопочных элементов указаны в табл. 3.9, а плоских - в табл. 3.10.

Таблица 3.9.

Обозначение габаритов	Диаметр, мм	Высота, мм
Цилиндрические		
AAA	8.2	40.2
AA	10.5	44.5
A	14.5	50.5

Кнопочные		
M5	7.86	3.56
M8	11.7	3.3
M15	11.7	5.34
M20	15.7	6.1
M30	16	11.1
M40	16	16.8

Таблица 3.10.

Обозначение габаритов	Длина, мм	Высота, мм	Ширина, мм
F15	14.2	3.02	14
F20	23.9	3.02	14
F25	22.6	5.85	22.6
F30	31.8	3.3	21.4
F40	31.8	5.35	21.4

Наиболее распространены ртутно-цинковые элементы. В них в качестве анода используются оксид ртути (HgO), катода - смесь порошка ртути и цинка или сплава индия с титаном, а электролита - 40% щелочь. Для малогабаритных приборов отечественной электропромышленностью созданы элементы типов РЦ-31С, РЦ-33С иРЦ-55УС с удельной энергией 600-700 кВт/м^3. Электрические параметры ряда отечественных ртутно-цинковых элементов и батарей, предназначенных для питания малогабаритных радиоэлектронных устройств, указаны в табл. 3.11.

Таблица 3.11.

Обозначение	Напряжение, В	Емкость, Ач	Ток разряда, мА	Габариты, мм	Масса, г
РЦ-31	1.25	0.07	1	11.5x3.6	1.3
РЦ-53	1.25	0.25	10	15.6x6.3	4.6
РЦ-55	1.25	0.5	10	15.6x12.5	9.5
РЦ-57	1.25	1.0	20	16x17	15
РЦ-59	1.25	3.0	60	16x50	44
РЦ-65	1.25	1.0	20	21x13	18.1
РЦ-75	1.25	1.5	30	25.5x13.5	27
РЦ-85	1.22	2.5	50	30.1x14	39.5
РЦ-93	1.25	13.0	300	31x60	170
2РЦ-55с	2.68	0.45	10	16.2x27	20
3РЦ-55с	4.02	0.45	10	16.2x40	30
4РЦ-55с	5.36	0.45	10	16.2x53	40
5РЦ-55с	6.7	0.45	10	16.2x66	50
6РЦ-63	7.2	0.6	10	23x48	71

Среди гальванических источников тока зарубежного производства широкое применение находят элементы фирм Duracell, Varta, Kodak. Технические характеристики малогабаритных гальванических элементов фирмы Duracell в табл. 3.12 .

Таблица 3.12.

Тип	Напряжение, В	Номинальная емкость, Ач	Диаметр, мм	Высота, мм
D392	1.5	0.05	7.9	3.6
D391	1.5	0.05	11.6	2.1
D389, D390	1.5	0.08	11.6	3.1
D386	1.5	0.12	11.6	4.2
D357H/10L14	1.5	0.17	11.6	5.4
LR54	1.5	0.04	11.6	3.0

LR43	1.5	0.08	11.6	4.2
LR44	1.5	0.10	11.6	5.4
DL2016	3.0	0.07	20.0	1.6
DL2032	3.0	0.18	20.0	3.2

Увеличения времени эксплуатации и повышения скрытности работы закладного устройства достигается путем обеспечения в нем автоматического подключения к источнику питания наиболее энергоемкого устройства - передатчика по акустическому или радиосигналу. В первом варианте в состав закладки включается устройство (акустоавтомат), подключающее к источнику питания передатчик при появлении на мембране микрофона акустического сигнала. В тишине, например, в ночное время во включенном состоянии (в “дежурном” режиме) находится лишь микрофонный усилитель с исполнительными электронным реле. При возникновении в помещении акустических сигналов от разговаривающих людей реле подключает передатчик и закладное устройство излучает радиосигналы с информацией. После прекращения разговора исходное состояние восстанавливается и излучение прекращается.

Во втором варианте закладные устройства дистанционно включаются на излучение по внешнему радиосигналу, подаваемому злоумышленником. Эти закладные устройства обеспечивают повышенную скрытность и более длительное время работы. Однако для их эффективного применения надо иметь дополнительный канал утечки сведений о времени циркулирования конфиденциальной информации в помещении, где установлено закладное устройство. Например, надо достаточно точно знать время, когда будут вестись в помещении конфиденциальные разговоры. Так как дистанционно-управляемые закладки содержат радиоприемник для приема управляющих радиосигналов. То они наиболее сложные и, следовательно, дорогие.

Рациональным решением задачи обеспечения закладных устройств электропитанием является подключение их к устройствам питания радио и электроприборов, в которые устанавливаются закладки. Широко применяются подобные закладные устройства в телефонных аппаратах, закамуфлированные под их элементы (конденсаторы, телефонные капсюли и др.), в тройниках для подключения нескольких приборов к одной розетке электросети. По оценке, приведенной в, в 75% закладных устройств используется автономное (батарейное) питание, 8% -питание от сети и 17% - питание от телефонной линии.

Следует отметить, что применяются, пока редко, также пассивные закладки, - без собственных источников электропитания. Для их активизации производится облучение их внешним электромагнитным полем частоты, соответствующей резонансной частоте колебательного контура закладки, образованного элементами ее конструкции. Модуляция радиосигнала производится в результате воздействия акустической волны на частотнозадающие элементы конструкции закладки.

Жесткие требования к габаритам, массе, энергопотреблению закладных устройств ограничивают мощности излучения их передатчиков. Наиболее часто (более 80%) применяются радиомикрофоны, мощность излучения которых находится в интервале 3-11 мВт, закладки с более высокой мощностью - до 22 мВт составляют менее 10%. Встречаются закладки и большей мощности излучения (до 200 мВт и более), однако их доля крайне незначительна. Малая мощность излучения передатчиков радиозакладок определяет относительно небольшую дальность приема их сигналов. Около 75% образцов обеспечивает функционирование канала на расстояниях 50-350м, 16% - на расстояниях 460-600 м, 7% - на расстояниях 740-800м и только около 2% - на расстояние до 1000 и более метров.

В общем случае технические данные закладных устройств находятся в следующих пределах:

- частотный диапазон - 27-900 МГц;

- мощность - 0.2-500 мВт;
- дальность - 10-1500 м;
- время непрерывной работы - от нескольких часов до нескольких лет;
- габариты - 1-8 дм3
- вес - 5-350 г

Основной проблемой оперативного применения закладных устройств является их рациональное размещение в помещении или в радиоэлектронном средстве. Рациональность достигается при обеспечении:

- поступления на вход закладки сигнала с уровнем, необходимым для качественной передачи звуковой или иной информации;
- скрытности размещения и работы закладки, по крайней мере, в течение времени подслушивания интересующей злоумышленника информации.

Эффективность выполнения этих условий зависит от удаленности места установки закладки от источников звука и наличия между ними звукопоглощающих и звукоизолирующих экранов, от чувствительности микрофона, размеров и параметров акустики, прежде всего, временем реверберации помещения и от времени, которым располагает злоумышленник для установки. Чувствительность современных малогабаритных микрофонов обеспечивают достаточно качественный прием акустических сигналов на удалении до 10 м при отсутствии экранов на пути распространения акустической волны.

Установка закладных устройств возможна с заходом злоумышленника в помещение, где производится их размещение, или без захода. Первый вариант позволяет более рационально разместить закладку как с точки зрения энергетики, так и скрытности, но связана с повышенным риском для злоумышленника. Поэтому в случаях, когда создаются предпосылки для дистанционной (беззаходовой) установки закладки, их забрасывают в помещение или ими выстреливают из пневматического ружья или лука. Например, комплект PS фирмы Sipe Electronic состоит из специального бесшумного пневматического пистолета с прицельным расстоянием 25 м и радиозакладкой, укрепленной на стреле. Стрела после выстрела надежно прикрепляется с помощью присоски к поверхностям из металла, дерева, пластмассы, бетона и других гладких строительных и облицовочных материалов. Микрофон обеспечивает съем речевой информации с расстояния до 10 м, а передатчик - ее передачу на расстояние до 100 м.

Несмотря на сравнительно малые габариты и вес закладных устройств они могут быть обнаружены при тщательном визуальном осмотре помещения. С целью продления времени их оперативного использования, а также приближения микрофонов к источнику звука закладные устройства камуфлируют под предметы, не вызывающие подозрение у окружающих людей. Трудно назвать предметы личного пользования, средства оргтехники, средства бытовой радиоэлектроники, в которые не вмонтировались бы различные устройства для подслушивания. Некоторые из таких средств подслушивания приведены в табл. 3.13.

Таблица 3.13.

Наименование	Тип, фирма	Характеристики
Радиопередатчики в:	ELECTRONIC:	
стакане	PK535	65x100 мм, 210 г, солнечные батареи
пепельнице	PK565-S	90x45 мм, 480 г, солнечные батареи
подсвечнике	PK580	100x175 мм, 650 г, солнечные батареи
калькуляторе	PK620-S	135x100 мм, радиус действия 150-200 м
розетке	PK550	140x60x40 мм, 380 г, дальность до 600 м
настольной зажигалке	PK575	80x32x52 мм, 150 г, время работы до 80 ч
лампочке	PK560	дальность до 250 м.
гвозде	PK520	35x6 мм, 96 г, 36 часов, до 200 м
шарик. ручке	PK585	135x11 мм, 25 г, 6 часов, до 300 м

часах	PK1025-S	88s108 или 130s150 МГц, 6 часов.
ремне	PK850-S	139 МГц, до 800 м.
Радиопередатчик в запонках, булавке для галстука	STG 4140, STG	15-150 МГц, мощность 5 мВт.
Радиопередатчик видеокассете	UM 007.3, SMIRAB ELECTRONIC	136-146 МГц, до 300 м, время непрырывной работы 3 суток
Магнитофон в книге	PK660, ELECTRONIC	200x250x65 мм, 1200 г, время записи 2x90 мин.
Магнитофон в пачке сигарет	PK1985, ELECTRONIC	55x87x21 мм, 160 г, время работы 11ч.

Средства лазерного подслушивания

Лазерное подслушивание является сравнительно новым методом подслушивания (первые рабочие образцы появились в 60-е годы), и предназначено для съема акустической информации с плоских вибрирующих под действием акустических волн поверхностей. К таким поверхностям относятся, прежде всего, стекла закрытых окон.

Система лазерного подслушивания состоит из лазера в инфракрасном диапазоне и оптического приемника. Лазерный луч с помощью оптического прицела направляется на окно помещения, в котором ведутся интересующие злоумышленника разговоры. При отражении лазерного луча от вибрирующей поверхности происходит модуляция акустическим сигналом угла отраженного луча лазера или его фазы.

В варианте угловой модуляции вектор отраженного от колеблющейся поверхности стекла меняется в соответствии с амплитудой акустической волны. Отраженный луч принимается оптическим приемником, размещаемым в соответствии с усредненным углом отражения. Положение светочувствительного элемента (фотокатода) оптического приемника юстируется таким образом, чтобы пятно отраженного лазерного луча при отсутствии колебаний стекла освещало половину экрана. В этом случае изменения направления отраженного луча при колебаниях стекла вызывают соответствующие изменения площади пятна света на фотокатоде оптического приемника и появление в светочувствительном слое модулированного по амплитуде электрического сигнала. Сигнал после усиления прослушивается и записывается на магнитную ленту. На практике юстировка производится по субъективному ощущению оператором разборчивости речи.

Второй вариант построения системы лазерного подслушивания предусматривает реализацию в оптическом приемнике фазовой демодуляции путем сравнения фаз облучающего и отраженного лучей. С этой целью исходный луч с помощью полупрозрачного зеркала расщепляется на два луча. Одним из них облучается стекло, другой направляется к приемнику в качестве опорного. В точке приема в результате интерференции опорного и отраженного лучей на поверхности светочувствительного слоя в нем возникают электрические заряды, величина которого соответствует разности фаз лучей. Второй вариант обеспечивает более высокую чувствительность системы подслушивания, но сложнее в реализации.

Примером системы лазерного подслушивания является система РК-1035 фирмы PK Electronic. Система состоит из лазерных передатчика и приемника, магнитофона для записи перехваченной информации. Передатчик и приемник системы устанавливаются на треноге. Лазерный передатчик имеет размеры 65x250 мм, вес 1.6 кг, мощность- 5 мВт, длина волны излучения- 850 мкм. Лазерный приемник имеет размеры 65x260 мм, вес 1.5 кг. Электропитание - от сети и автономное.

Данные о возможностях систем лазерного подслушивания противоречивые. В рекламных материалах дальность указывается для разных систем от сотен метров до км.

Однако без ссылки на уровень внешних акустических шумов эти величины можно рассматривать как потенциально достижимые в идеальных условиях. В городских условиях, когда принимаются дополнительные меры по звукоизоляции помещений от шума улицы, дальности будут существенно меньшими. Следует также иметь ввиду сложности практической установки излучателя и приемника, при которых обеспечивается попадание зеркально отраженного от стекла невидимого лазерного луча на фотоприемник. Уровни же диффузно отраженных от стекла лучей столь малы, что их не удается принять на фоне городских акустических шумов. Кроме того, следует отметить, что соотношение между стоимостью системам лазерного подслушивания и затрат на эффективной защиты от них не в пользу рассматриваемого метода добывания информации.

Следовательно, системы лазерного подслушивания, несмотря на их достаточно высокие потенциальные возможности имеют ограниченное реальное применение, в особенности разведкой коммерческих структур.

Средства высокочастотного навязывания

Добывание информации путем высокочастотного навязывания достигается в результате дистанционного воздействия высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать их информационные параметры первичными электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющие собой высокочастотные контура с распределенными параметрами и объем которых меняется под действием акустической волны. Если частота такого контура совпадает с частотой высокочастотного навязывания, а поверхность полости находится под воздействием акустической информацией, то эквивалентный контур переизлучает и модулирует внешнее поле.

Более часто в качестве модулирующего применяется нелинейный элемент, в том числе в схеме телефонного аппарата. В этом случае высокочастотное навязывание обеспечивается подведением к телефонному аппарату высокочастотного гармонического сигнала путем подключения к телефонному кабелю высокочастотного генератора. В результате взаимодействия высокочастотного колебания с речевыми сигналами на нелинейных элементах телефонного аппарата происходит модуляция высокочастотного колебания речевым низкочастотным сигналом. Принципы этого явления аналогичны работе смесителя радиоприемника. После преобразования появляются сигналы, частоты которых представляют различные комбинации частот исходных сигналов. Эти сигналы модулированы сигналами речевой информации и могут перехвачены приемником злоумышленника.

3.4. Способы и средства добывания информации о радиоактивных веществах

Добыванием информации о радиоактивных веществах занимается радиационная разведка. Для обнаружения радиоактивных излучений она использует специальные дозиметрические приборы. Структура типового прибора радиационной разведки приведена на рис. 3.16.

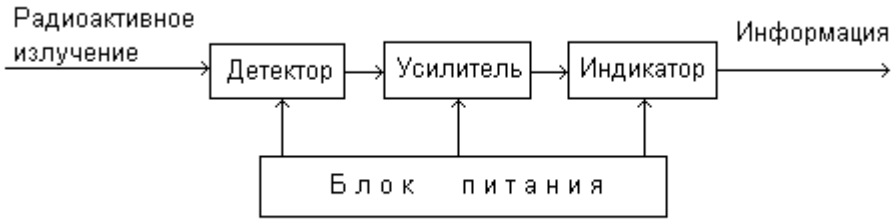


Рис. 3.16. Структура прибора радиационной разведки.

Детектор преобразует энергию радиоактивного излучения в электрические сигналы, которые после усиления поступают на стрелочный или цифровой индикатор. В качестве детектора используются ионизационные камеры, газоразрядные и сцинтилляционные счетчики, кристаллы полупроводника, фотопленка,

Ионизационные камеры (Вильсона, пузырьковые, искровые) представляют сосуд цилиндрической или прямоугольной формы, заполненные газом с пересыщенным паром (в камере Вильсона), жидким водородом (в пузырьковой камере) и инертным газом (в искровой камере). В искровой камере имеются, кроме того, плоскопараллельные близко расположенные друг к другу пластины, на которые подается высокое напряжение, чуть ниже пробойного. Когда через камеру Вильсона и пузырьковую камеру пролетает электрически заряженная частица, на возникаюших на ее пути ионах конденсируются маленькие капельки жидкости, видимые при боковом освещении. При пролете быстрой частицы через искровую камеру вдоль ее траектории между пластинами проскакивают искры, создавая огненный трек.

В малогабаритных приборах радиационной разведки применяются в основном газоразрядные счетчики (счетчики Гейгера-Мюллера). Газоразрядные счетчики представляют собой стеклянную герметичную трубку, заполненную смесью газовой смесью (аргона и воздуха, аргона и паров и др.) под давлением 0.1 атмосферы. Внутренняя поверхность трубки металлизирована. Внутри трубки протянута металлическая нить, на которую подается высокое положительное напряжение 1000-1500 В постоянного тока, а к поверхности счетчика - отрицательное напряжение. Когда в газоразрядную трубку попадает ионизирующая частица, происходит лавинообразный процесс образования ионов, между электродами возникает короткий импульс тока, который подается на вход усилителя. В результате вторичной ионизации обеспечивается высокая чувствительность детектора. Импульсы тока усиливаются и регистрируются в простейшем варианте в виде звуковых щелчков, в более совершенных дозиметрических приборов частость импульсов преобразуется в значение уровня излучения, отображаемое с помощью стрелочных или цифровых индикаторов.

Счетчики Гейгера-Мюллера для регистрации α-излучения имеют очень тонкое (0.002-0.003 мм) слюдяное окно, через которое частицы без существенного поглощения попадают в трубку. Для регистрации β- излучения окно трубки делают из алюминиевой фольги толщиной 0.1-0.2 мм, которая поглощает α-частицы. Трубки для регистрации γ-излучения закрыты слоем алюминия толщиной 1 мм, поглощающей β- излучение.

Сцинтиляционные детекторы представляют собой экран (пластину) из стекла, покрытый флюоресцирующим веществом (сульфидом цинка, антраценом или другими веществами, преобразующими кинетическую энергию радиоактивных частиц в энергию световой вспышки). Путем размещения за экраном фотоумножителя вспышки света могут преобразовываться в электрические сигналы с последующим измерением их интенсивности электронным счетчиком. Преимущество сцинтилляционного детектора состоит в том, что он может раздельно считать частицы, поступающие через очень короткие промежутки времени (10^{-8}-10^{-9} с вместо 10^{-5}-10^{-6} с у счетчиков Гейгера-Мюллера). Дальнейшим развитием сцинтилляционного счетчика является люминисцентная камера, которая не только считает частицы в течение очень короткого

времени (10^{-13}-10^{-14} с), но и с помощью соответствующего электронно-оптического устройства регистрирует их траектории.

Широкое распространение получили кристаллические полупроводниковые детекторы, основу которых составляют полупроводниковый кристалл кремния или германия с различными добавками. Электропроводность кристалла изменяется под действием ионизирующего излучения.

В качестве фотодетекторов применяют также рентгеновскую фотопленку, по степени почернения которой за определенное время судят об уровне излучения.

Приборы для обнаружения и измерения радиоактивных излучений в зависимости от назначения делятся на индикаторы радиоактивности, радиометры и дозиметры. По способу индикации интенсивности излучения - на стрелочные и цифровые.

Индикаторы излучений информируют оператора световой или звуковой индикацией о наличии в зоне поиска радиоактивных веществ, радиометры предназначены для обнаружения и измерения радиоактивного заражения среды, а дозиметры - для измерения дозы облучения.

Величина, которую измеряют радиометры, называют мощностью экспозиционной дозы (МЭД) гамма-излучения. Экспозиционная доза γ-излучения равна отношению заряда, созданного гамма-квантами в воздухе при нормальных условиях, к массе этого воздуха. В качестве единицы измерения в системе СИ принята мера в кулон/кг (Кл/кг). Широко применяется несистемная единица измерения - рентген и ее доли (миллирентген и микрорентген). Соотношение между этими единицами равно: $1Р=2.58\cdot 10^{-4}$ Кл/кг.

Мощностью экспозиционной дозы называется величина экспозиционной дозы в единицу времени. Фоновая мощность излучения космоса и радионуклидов земли составляет в среднем 5-30 мкР/ч. Энергия α и β-частиц оценивается также в электрон-вольтах (эВ) и см пробега Один эВ равен кинетической энергии, получаемой электроном под действием разности потенциалов 1 В. Энергия альфа-частиц, излучаемых различными естественными радиоактивными элементами, составляет 4-9 МэВ (1 МэВ $=10^6$ эВ). что обеспечивает их пробег ав атмосфере воздуха при нормальных условиях 2.5-8.6 см.

На рынке имеются разнообразные радиометры, в том числе бытовые «Белка», «Эксперт», «Сосна» и другие. Разнообразные прфессиональные приборы выпускает Обнинский приборный завод “ Сигнал”. Например, измеритель мощности дозы гамма-излучения ИМД-2 применяется в стационарных условиях, на летательных аппаратах, подвижных объектах и для пешей разведки, Индикация уровня производится с помощью светящегося сектора на шкале прибора. Он имеет следующие характеристики:

- диапазон измерения МЭД.....10 мкР/ч-1000 Р/ч;
- погрешности измерения.....30 %;
- диапазон температур окружающей среды, ^{0}С ..... -50...+50;
- вес прибора, кг .....1.6 кг;
- габариты, мм ..... 198x180x82.

Величина поглощения энергии излучения в единице биологической массы (ткани) называется основной дозиметрической величиной (дозой). Единица измерения дозы в системе СИ - зиверт (Зв) и несистемная единица измерения - бэр, причем 1 бэр=100 Зв.

По биологическому воздействию поглощенная биологической тканью доза, измеренная в бэрах, примерно равна экспозиционной дозе, измеренной в рентгенах. Поэтому уровни радиоактивного заражения оценивают как в рентгенах, так и бэрах.

Малогабаритные дозиметры (ДРС-01, ДКС-04, ДЭГ-8,ДРГ-01Т1, ДРГ-05М и др.) постоянно применяются людьми, имеющие дело с радиоактивными веществами, для измерения принятой ими дозы в течение определенного времени работы, например, месяца. Пороговое значение дозы за год не должно превышать 5 бэр.

Глава 4. Технические каналы утечки информации

Информация, записанная на распространяющихся в пространстве носителях, может быть перенесена этими носителями от источника к несанкционированному получателю. В таком случае говорят об утечке информации по аналогии с утечкой жидких или газообразных веществ. Однако по сравнению с ними утечка информации имеет ряд особенностей.

4.1. Особенности утечки информации

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Понятие "утечка" широко распространено, Говорят об утечке воды, газа, материальных ценностей со склада, информации из различных структур и т. д. Утечка информации возможна путем ее разглашения людьми, утерей ими носителей с информацией, переносом информации с помощью полей, потоков элементарных частиц, веществ в газообразном, жидком или твердом виде. Например, желание сотрудников поделиться последними новостями о работе с родными или близкими создают возможности утечки конфиденциальной информации. Переносчиками информации могут быть любые ее носители.

Часто под утечкой понимают случайный процесс, вроде вытекания воды из неисправного крана. Такой подход представляется упрощенным. В криминальной практике известны факты организации утечки, например, бензина с последующим списыванием его на случайную неисправность в нефтепроводе или хранилище. Практикуются в политической жизни общества организация утечки информации из правительственных структур с целью зондирования или подготовки общественного мнения перед принятием непопулярных решений.

Утечка информации по сравнению с утечкой (хищением) материальных объектов имеет ряд особенностей, которые надо учитывать при организации защиты информации:

- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличии, например, от утечки воды или газа.
- при утечке информации происходит ее тиражирование, которое не изменяет характеристики носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие демаркирующие признаки продукции и т. д.);
- цена информации при ее утечке уменьшается за счет тиражирования;
- факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности принимать могут оказаться неэффективными;

Первая особенность имеет существенное значение для безопасности информации, так как сами по себе факты утери документа, разглашения сведений, распространения носителей за пределы контролируемой зоны и другие действия далеко не всегда приводят к утечке информации. Например, если конфиденциальный разговор во время совещания в кабинете руководителя организации слышен в приемной из-за неплотно закрытой двери, а в приемной нет людей, то утечки информации нет, хотя носитель информации (акустическая волна) выходит за пределы контролируемой зоны - помещения. Если в приемной находится добросовестно выполняющий свои обязанности секретарь руководителя, который после совещания будет оформлять его результаты, то утечка информации также отсутствует, так как информации не попадет к злоумышленнику. Только в том случае, когда в приемной будет находиться сотрудник организации или посетитель, который воспользуется информацией из услышанного

разговора в личных целях или поделиться ею с другими заинтересованными в ней людьми, то происходит утечка информации из кабинета руководителя. В общем случае можно говорить об утечке информации как факте нарушения ее безопасности только в том случае, если она попадает к злоумышленнику независимо от того, знает или не знает об этом владелец информации. Если по какой-то причине на этом пути передачи информации происходит разрыв в цепочке, то информация исчезает вместе с ее носителем, а утечки информации не происходит.

Следовательно, под утечкой следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда информация попадает к злоумышленнику. Выход же носителя за пределы заданной области создает предпосылки для утечки информации и повышает угрозу ее безопасности.

Замечание о несанкционированности получателя имеет также принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Часто хищение и утечку информации рассматривают как автономные процессы. Если под хищением понимать умышленное присвоение чужой собственности без разрешения ее законного владельца, то утечка информации представляет собой один из способов ее хищения. Действительно, если человек на государственной земле находит клад, слиток из драгоценных металлов или драгоценный камень, которые по закону являются собственностью государства, то он обязан их сдать соответствующему государственному органу. В противном случае его действия классифицируются как хищение и он может быть привлечен к ответственности. Аналогичная ситуация с утечкой информации. Когда злоумышленник находит утерянный документ с грифом “секретно” и сознательно продает его зарубежной спецслужбе, то он привлекается к уголовной ответственности за хищение государственной тайны.

Физический путь переноса информации от ее источника к несанкционированному получателю называется каналом утечки. Если запись информации на носитель канала утечки и съем ее с носителя производится с помощью технических средств, то такой канал называется техническим каналом утечки.

Несанкционированный перенос информации полями различной природы, макро- и микрочастицами производится в рамках технических каналов утечки информации.

4.2. Характеристики технических каналов утечки информации

Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать 3 основные элемента: источник сигнала, среду распространения носителя и приемник. Обобщенная типовая структура канала передачи информации приведена на рис. 4.1.

Рис. 4.1. Структура канала передачи информации.

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода

предыдущего канала. В качестве источника сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией;

Указанные на рисунке стрелками пути входа и выхода информации обозначают вход и выход первичных сигналов с информацией. Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Кроме того, он выполняет следующие функции:

- создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;
- производит запись информации на носитель (модуляцию информационных параметров носителя);
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Запись информации производится путем изменения параметров носителя в соответствии с уровнем первичного сигнала, поступающего на вход. Если носителями информации являются субъекты и материальные тела (макрочастицы), то передатчик соответствует первоначальному смыслу этого слова - передавать или переносить, т. е. выполняет функцию носителя. В случае когда информацию переносят сигналы (поля, электрический ток и элементарные частицы), то передатчики являются источниками сигналов.

Источниками сигналов могут быть как источники функциональных каналов связи, так и опасных сигналов. К опасным сигналам относятся сигналы с конфиденциальной информацией, появление которых является для источника информации случайным событием и им не контролируется.

Среда распространения носителя - часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя с информацией. Основными, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления (или пропускания энергии) сигнала на единицу длины;
- частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала);
- вид и мощность помех для сигнала.

Приемник выполняет функцию, обратные функции передатчика. Он производит:

- выбор (селекцию) носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съем информации;
- съем информации с носителя (демодуляцию, декодирование);
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного восприятия ими.

Если получатель информации человек, то информация с выхода приемника должна быть представлена на языке общения людей; если техническое устройство, то форма представления информации должна быть понятна этому устройству. Например, если

получатель - ЭВМ, то с выхода приемника на ЭВМ подается двоичная последовательность в кодах, например, таблицы ASCII.

Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель санкционированный, то канал функциональный, в противном случае - канал утечки. Классификация каналов утечки информации дана на рис. 4.2.

Рис. 4.2. Классификация каналов утечки информации.

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя. По этому признаку они делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле в диапазоне 0,46-0,76 мкм (видимый свет) и 0.76-13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам из меди, железа, алюминия. Диапазон колебаний этого вида носителя чрезвычайно велик: от звукового диапазона до десятков ГГц. Часто этот канал называют электромагнитным, что представляется недостаточно корректным, так как носителями информации в оптическом канале являются также электромагнитные поля, но в более высокочастотном диапазоне. Кроме того, широко используется в качестве носителя информации модулированный поток электронов (электрический ток). Объединяя эти два носителя информации в канале одного вида, целесообразно назвать его «радиоэлектронный» (электромагнитное поле в радиодиапазоне и электроны электрического тока).

Носителями информации в акустическом канале являются механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц - 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы организации вещественных носителей с секретной или конфиденциальной информацией, прежде всего, выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат химические элементы, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

Когда речь идет о распространении за пределы организации отходов производства в широком смысле, то следует отличать технический канал утечки от агентурного, в рамках которого вынос носителя с информацией производится проникшим к источнику злоумышленника, завербованным сотрудником организации или сотрудником,

стремящимся продать информации любому ее покупателю. Граница между каналами достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом материально-вещественном канале - носители вывозятся из организации с целью освобождения ее от отходов или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие газообразные отходы, или водные потоки рек или водоемов, куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от распространения в них.

По информативности каналы утечки делятся на информативные, малоинформативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Периодический канал утечки может возникнуть при условии, например, размещения во дворе не укрытой продукции, демаскирующие признаки о которой составляют тайну, во время пролетов разведывательных космических аппаратов. К эпизодическим каналам относятся каналы, утечка информации в которых имеет разовый случайный характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем - по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому - путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка - среда распространения - радиоприемник) каналов. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно разместить ретранслятор в портфеле, сдаваемый якобы на хранение в камеру хранения закрытого предприятия.

Как любой канал связи канал утечки информации характеризуется следующими основными показателями:

- пропускной способностью;
- дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по каналу в единицу времени с определенным качеством. В теории связи пропускная способность канала в бодах (битах в секунду) определяется по формуле:

$$C=\Delta F \log_2 (1+P_c/P_п),$$

где ΔF-ширина полосы пропускания канала связи;

P_c и $P_п$ - мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Следовательно, пропускная способность канала связи является интегральной характеристикой, учитывающей как ширину полос частот сигнала, которую пропускает

канал, так и его энергетику. Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации.

По ширине полосы частот пропускания каналы делятся на узкополосные и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300-3400 Гц и относится к узкополосным, шириной 8 МГц для передачи телевизионных сигналов - к широкополосным. Чем шире канал, тем больше информации можно передать за единицу времени. Так как для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально-допустимое для каждого вида информации и носителя отношение сигнал/помеха, то это отношение достигается на различном удалении от источника сигнала, в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей - электромагнитная волна в длинноволновом диапазоне частот.

4.3. Оптические каналы утечки информации

Структура оптического канала утечки информации имеет вид, показанный рис. 4.3.

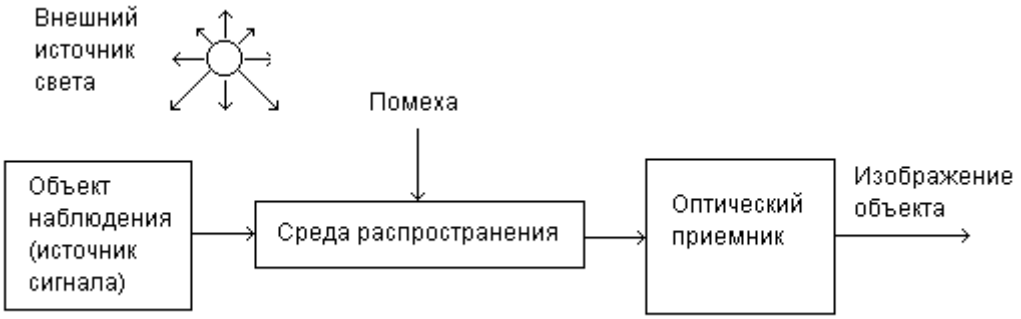


Рис. 4.3. Структура оптического канала утечки информации.

Объект наблюдения в оптическом канале утечки информации является одновременно источником информации и источником сигнала в том смысле, что световые лучи, несущие информацию о видовых признаках объекта, представляют собой отраженные объектом лучи внешнего источника или его собственные излучения.

Отраженный от объекта свет содержит информацию о его внешнем виде (видовых признаках), а излучаемый объектом свет - о параметрах излучений (сигнальных признаках). Запись информации производится в момент отражения падающего света путем изменения яркости и спектрального состава отраженного луча света. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения.

В общем случае объект наблюдения излучает электромагнитные волны и отражает свет другого источника как в видимом, так и ИК-диапазонах. Однако в конкретных условиях соотношения между мощностью собственных и отраженных излучений в видимом и ИК-диапазонах существенно отличаются.

В видимом диапазоне мощность излучения определяется в подавляющем большинстве случаев мощностью отраженного света и содержащихся в объекте искусственных источников света. Например, габариты автомобиля в ночное время обозначаются включенными фонарями красного цвета, укрепленными по краям автомобиля. Объект наблюдения или его элементы излучают собственные электромагнитные излучения в видимом диапазоне, вызванные тепловым движением электронов, при высокой температуре. В ближней (0.75-3 мкм) и средней (3-6 мкм)

диапазонах ИК-излучения объектов значительно меньше мощности отраженного от объекта потока солнечной энергии. Однако с переходом в длинноволновую область ИК-излучения мощность теплового излучения объектов может превышать мощность отраженной солнечной энергии. Основным и наиболее мощным внешним источником света является Солнце. При температуре поверхности около 6000^0 Солнце излучает огромное количество энергии в достаточно широкой полосе частот - от ультрафиолетового до инфракрасного (0.17-4 мкм). Максимум солнечного излучения приходится на 0.47 мкм, в ультрафиолетовой части оно резко убывает, в инфракрасной - регистрируется в виде широкой и пологой кривой.

При прохождении через атмосферу солнечные лучи взаимодействуют с содержащими в ней молекулами газов, частицами пыли, дыма, кристалликами льда, каплями воды. В результате такого взаимодействия часть солнечной энергии поглощается, другая - рассеивается.

Процессы рассеяния и поглощения солнечной энергии уменьшают интенсивность солнечной радиации на поверхности Земли и меняют спектр солнечного света, освещающего наземные объекты. В кривой излучения этого света, характеризующей интенсивность излучения в зависимости от длины волны, появляются участки поглощения и пропускания. Последние называются окнами прозрачности. Излучения длиной менее 0.27 полностью поглощаются озоном. Атмосферное рассеяние света уменьшает прямую солнечную радиацию и повышает рассеянное (диффузное) излучение атмосферы. Рассеяние в коротковолновой части спектра сильнее, чем в длинноволновой. Особенно сильно оно в голубой и ультрафиолетовой областях, Поэтому небо имеет голубой цвет. Интенсивность рассеяния солнечного света в ближнем инфракрасном диапазоне незначительная.

Задымленность приповерхностного слоя атмосферы мало влияет на излучения ближнего ИК-диапазона, если размеры твердых частиц дыма в атмосфере не превышают 1 мкм. Туман и облака очень сильно рассеивают ИК-излучение в этом интервале длин, так как водяные капли и имеют размер около 4 мкм. Молекулярное и аэрозольное рассеяние солнечного света вызывает ее свечение, которое называют дымкой. Рассеянное излучение создает освещенность теневых участков земной поверхности, увеличивая их относительную яркость.

Облачность существенно влияет на суммарную освещенность. Наличие облачности высоких ярусов, не закрывающих солнечный диск, повышает рассеянное излучение и при сохранении значения прямой освещенности увеличивает суммарную величину на (20-30)% по сравнению с освещенностью при безоблачном небе. Низкая облачность так же, как и тени облаков, снижают суммарную освещенность в 2-5 раз, в зависимости от высоты Солнца. При снежном покрове и облачности многократное отражение ими излучения повышает суммарную освещенность, особенно в теневых участках.

Освещенность в дневное время земной поверхности Солнцем составляет в зависимости от его высоты, облачности атмосферы 10^4 - 10^5 лк. С движением Солнца к горизонту Земли, когда зенитное расстояние между ними достигает максимума, освещенность, создаваемая Солнцем, составляет приблизительно 10 лк. При этом изменяется и спектр солнечного света, так как при прохождении толщи атмосферы синие и фиолетовые лучи ослабеваются сильнее, чем оранжевые и красные, вследствие чего максимум излучения Солнца смещается в красную область цвета. С заходом Солнца за горизонт и наступлением сумерек освещенность убывает вплоть до наступления астрономических сумерек, за которыми следует наиболее темное время суток - ночь.

В лунную ночь при безоблачном небе, когда так называемую естественную ночную освещенность (ЕНО) создает отраженный от Луны солнечный свет составляет около 0.3 лк в полнолуние. Величина ЕНО, создаваемая светом Луны, в течение месяца меняется приблизительно в 100 раз в зависимости от взаимного положения Луны, Солнца и Земли. Лунный месяц разделяется по уровню освещенности на четыре части, каждая

длительностью около недели.

Источниками излучения в безлунную ночь при безоблачном небе, называемым звездным светом, являются солнечный свет, отраженный от планет и туманностей, свет звезд, а также свечение кислорода и азота в верхних слоях атмосферы на высоте 100-300 км. Освещенность поверхности Земли звездным светом составляет в среднем 0.001 лк.

В инфракрасном диапазоне мощность излучения объекта зависит от температуры тела или его элементов, мощности падающего на объект света и коэффициента отражения объекта в этом диапазоне. Коэффициент теплового излучения для реальных объектов не постоянен по спектру и определяется в соответствии с законом Кирхгофа отношением спектральной плотности энергетической яркости объекта к спектральной плотности энергетической яркости абсолютно черного тела. Абсолютно черное тело обладает максимумом энергии теплового излучения по сравнению со всеми другими источниками при той же температуре.

Средняя температура поверхности Земли близка к 17 градусов по Цельсию. Максимум ее вторичного теплового излучения приходится на 9.7 мкм. Объекты под действием солнечной радиации в течение дня по-разному отдают накопленное тепло в окружающее пространство. Различия в температуре излучения могут рассматриваться как демаскирующие признаки.

Объекты могут иметь собственные источники тепловой энергии, например, высокотемпературные элементы машин, дизель-электростанции и др., температура которых значительно выше температуры фона. Максимум теплового излучения таких объектов смещается в коротковолновую область, что служит демаскирующим признаком для таких объектов.

Длина (протяженность) канала утечки зависит от мощности света от объекта, свойств среды распространения и чувствительности фотоприемника. Среда распространения в оптическом канале утечки информации возможна трех видов:

- безвоздушное (космическое) пространство;
- атмосфера;
- оптические световоды.

Оптический канал утечки информации, среда распространения которого содержит участки безвоздушного пространства, возникает при наблюдении за наземными объектами с космических аппаратов. Граница между космическим пространством и атмосферой достаточно условна. На высотах 200-300 км существуют еще остатки газов, проявляющиеся в тормозящем действии на космические аппараты.

Сложный состав атмосферы определяет ее пропускные способности. В общем случае прозрачность атмосферы зависит от соотношения длины проходящего сквозь нее излучений и размеров взвешенных в атмосфере частиц. Если размеры частиц соизмеримы с длиной волны света (больше половины длины волны), то пропускание значительно ухудшается. Уровень пропускания меняется в зависимости от длины световой волны.

В видимой области прохождению света препятствуют абсорбирующие молекулы кислорода и воды. Коэффициент пропускания в ней немногим более 60%. В ближней ИК-области пропускание несколько большее - до 70%. Адсорбентом в этой области являются пары воды. В средней ИК-области, в диапазоне 3-4 мкм, пропускание достигает почти 90%. Высокое пропускание имеет довольно обширный участок в дальней ИК-области (8 до 13 мкм). Абсорбентом в нем являются молекулы кислорода и воды, а также углекислого газа и озона в атмосфере.

Метеорологическая видимость даже в окнах прозрачности зависит от наличия в атмосфере взвешенных частиц пыли и влаги, образующих мглу и туман, капелек и кристаллов воды в виде дождя и снега, а также аэрозолей и дымов, содержащих твердые частицы. Все это вызывает замутнение атмосферы и ухудшает видимость. Прозрачность атмосферы как канала распространения света оценивается метеорологической дальностью

видимости. Под последней понимается предельно большое расстояние, начиная с которого при данной прозрачности атмосферы в светлое время суток абсолютно черный предмет с угловыми размерами 20'x20' сливается с фоном у горизонта и становится невидимым. В зависимости от состояния атмосферы дальность видимости, определяющая протяженность оптического канала утечки, имеет значения, приведенные в табл. 4.1.

Таблица 4.1.

Метеорологическая дальность видимости, км	Оценка видимости, балл	Визуальная оценка замутненности атмосферы и видимости
Менее 0.05	0	Очень сильный туман
0.05 - 0.2	1	Сильный туман
0,2 - 0.5	2	Умеренный туман
0.5 - 1.0	3	Слабый туман
1.0 - 2.0	4	Очень сильная замутненность (очень плохая видимость)
2.0 - 4.0	5	Сильная замутненность (плохая видимость)
10.0	6	Умеренная замутненность (умеренная видимость)
20.0	7	Удовлетворительная видимость
50.0	8	Хорошая видимость
Более 50.0	9	Исключительно хорошая видимость
Около 300	10	Чистый воздух

Использование метеорологической дальности для оценок прозрачность атмосферы удобно тем, что ее величина периодически определяется на станциях метеорологической службы. Оценка видимости оценивается в метрах или в баллах и передается радиостанциями. Если объект наблюдения и наблюдатель находятся на земле, то протяженность канала утечки определяется не только состоянием атмосферы, но и ограничивается влиянием кривизны Земли. Дальность прямой видимости $Д_{пр}$ в км с учетом кривизны Земли можно рассчитать по формуле:

$$D_{пр} = 3.57(\sqrt{h_o} + \sqrt{h_н}),$$

где h_o - высота размещения объекта над поверхностью Земли в м;

$h_н$ - высота расположения наблюдателя над поверхностью Земли в м.

Например, для h_o=3 м и $h_н$=5 м $D_{пр}$=14 км, что меньше метеорологической дальности при хорошей видимости. Эта формула не учитывает неровности Земли и различные инженерные сооружения (башни, высотные здания и т. д.), создающие препятствия для света.

К свойствам среды распространения, влияющих на длину канала утечки, относятся:

- характеристики прозрачности среды распространения;
- спектральные характеристики света.

Ослабление света при прохождении через атмосферу характеризуется коэффициентом пропускания атмосферы.

Типовые варианты оптических каналов утечки информации приведены в табл. 4.2.

Таблица 4.2.

Объект наблюдения	Среда распространения	Оптический приемник
Документ, продукция в помещении	Воздух Воздух + стекло окна	Глаза человек + бинокль, фотоаппарат
Продукция во дворе, на машине, ж/платформе	Воздух Атмосфера + безвоздушное пространство	То же Фото, ИК, телевизионная аппаратура на КА
Человек в помещении, во дворе, на улице	Воздух Воздух + стекло	Глаза человека+бинокль, фото, кино, телев. ап-ра

До недавнего времени атмосфера и безвоздушное пространство были единственной средой распространения световых волн. С разработкой волоконно-оптической технологии появились направляющие линии связи в оптическом диапазоне, которые в силу огромных их преимуществ по отношению к традиционным электрическим проводникам рассматриваются как более совершенная физическая среда для передачи больших объемов информации. Линии связи, использующие оптическое волокно, устойчивы к внешним помехам, имеют малое затухание, долговечны, обеспечивают значительно большую безопасность передаваемой по волокну информации.

Волокно представляет нить диаметром около 100 мкм, изготовленного из кварца на основе двуокиси кремния. Волокно состоит из сердцевины и оболочки с разными показателями преломления. Для передачи сигналов применяются два вида волокна: одномодовое и многомодовое.

В одномодовом волокне световодная жила имеет диаметр порядка 8-10 мкм, по которой может распространяться только один луч (одна мода). В многомодовом волокне диаметр световодной жилы составляет 50-60 мкм, что делает возможным распространение в нем большого числа лучей (много мод).

Любое волокно характеризуется двумя важнейшими параметрами: затуханием и дисперсией. Затухание измеряется в децибелах на километр (дБ/км) и определяется потерями на поглощение и рассеяние излучения в оптическом волокне. Потери на поглощение зависят от чистоты материала, а потери на рассеяние - от неоднородностей его показателя преломления. Лучшие образцы волокна имеют затухание порядка 0.15-0.2 дБ/км, разрабатываются еще более « прозрачные» волокна с теоретическим пределом затухания порядка 0.02 дБ/км для волны длиной 2.5 мкм. При таком затухании сигнала могут передаваться на расстояние в сотни км без ретрансляции.

Дисперсия, т. е. зависимость скорости распространения сигналов от длины волны, ухудшает качество сигнала, следовательно, информации на выходе длинного световолокна. Так как светодиод или лазер, являющиеся источниками сигнала для этой среды распространения, излучают некоторый спектр длин волн, дисперсия приводит к расширению импульсов при их распространению по волокну и тем самым к искажению сигналов. Дисперсия ограничивает дальность передачи и верхнее значение частоты передаваемого сигнала.

Волокна объединяют в волоконно-оптические кабели, покрытые защитной оболочкой. По условиям эксплуатации кабели подразделяются на монтажные, станционные, зоновые и магистральные. Кабели первых двух типов используются внутри зданий и сооружений. Зоновые и магистральные кабели прокладываются в колодцах кабельных коммуникаций, в грунтах, на опорах, под водой.

Хотя возможность утечки информации из волоконно-оптического кабеля существенно ниже, чем из электрического, но при определенных условиях такая утечка возможна. Для съема информации в месте доступа к кабелю разрушают его защитную оболочку, прижимают фотодетектор приемника к очищенной площадке и изгибают кабель на угол, при котором часть световой энергии направляется на фотодетектор приемника.

4.4. Радиоэлектронные каналы утечки информации

В радиоэлектронном канале передача носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;

- высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);

- большой объем добываемой информации;

- оперативность получения информации вплоть до реального масштаба времени;

- скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация, видовые и сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

Структура радиоэлектронного канала утечки информации в общем случае включает (см. рис. 4.4) источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала.

Рис. 4.4. Структура радиоэлектронного канала утечки информации.

В радиоэлектронных каналах утечки информации источники сигналов могут быть четырех видов:

- передатчики функциональных каналов связи;

- источники опасных сигналов;

- объекты, отражающие электромагнитные волны в радиодиапазоне;

- объекты, излучающие собственные (тепловые) радиоволны.

Средой распространения радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство и направляющие - электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле - в атмосфере, в безвоздушном пространстве или по направляющим - волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации - демодуляция.

При перехвате сигналов функциональных каналов связи передатчики этих каналов являются одновременно источниками радиоэлектронных каналов утечки информации. В общем случае направления распространения электромагнитной волны от передатчика к санкционированному получателю и злоумышленнику отличаются. В функциональных каналах связи максимум излучения энергии электромагнитной волны ориентируют в направлении расположения приемника санкционированного получателя. Поэтому мощность источника сигналов радиоэлектронного канала утечки информации, как правило, существенно меньше мощности излучения в функциональном канале связи.

В зависимости от способа перехвата информации различают два вида радиоэлектронного канала утечки информации.

В канале утечки 1-го вида производится перехват информации, передаваемой по функциональному каналу связи. С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала функционального радиоканала или подключается (контактно или дистанционно) к проводам соответствующего функционального канала. Такой канал утечки информации имеет общий с функциональным каналом источник сигналов - передатчик. Так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то среды распространения сигналов в них от общего передатчика различные или совпадают, например, до места подключения приемника злоумышленника к проводам

телефонной сети.

Радиоэлектронный канал утечки 2-го вида имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов. Передатчик этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. В качестве такого передатчика применяются источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают на базе акустоэлектрических преобразователей, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Опасные сигналы создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил эксплуатации, не учете полей вокруг средств или токонесущих проводов при их прокладке в здании и т. д.

Вариантов условий для возникновения опасных сигналов очень много. Например, в усилительных каскадах любого радиоэлектронного средства (радиоприемника, телевизора, радиотелефона и др.) могут возникнуть условия для генерации сигналов на частотах вне звукового диапазона, которые модулируются электрическими сигналами акустоэлектрических преобразователей. Функции акустоэлектрических преобразователей могут выполнять элементы (катушки индуктивности, конденсаторы) генераторов, являющихся функциональными устройствами.

Особенностью передатчиков этого канала является малые амплитуда электрических сигналов - единицы и доли мВ, и мощность радиосигналов, не превышающая десятки мВт (для радиозакладок). В результате этого протяженность таких каналов невелика и составляет десятки и сотни метров. Поэтому для добывания информации с использованием такого канала утечки информации приемник необходимо приблизить к источнику на величину длины канала утечки или установить ретранслятор. Среда распространения и приемники этого вида каналов не отличаются от среды и приемников каналов 1-го вида.

Электрические сигналы как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков до миллиардов Гц.

Наиболее широко применяются сигналы, ширина спектра которых соответствует ширине спектра стандартного телефонного канала. Такие сигналы передают речевую информацию с помощью телефонных аппаратов и распространяются по направляющим линиям связи, связывающих абонентов как внутри предприятия (организации), так внутри населенного пункта, города, страны, земного шара в целом.

В общем случае направляющие линии связи создаются для передачи сигналов в заданном направлении с должным качеством и надежностью. Способы и средства передачи электрических сигналов по проводам рассматриваются прикладной области радиотехники, называемой проводной связью.

Различают воздушные и кабельные проводные линии связи. Воздушные линии связи относятся к симметричным цепям, отличительной особенностью которых является наличие двух проводников с одинаковыми электрическими свойствами.

В зависимости от типа несущих конструкций они делятся на столбовые и стоечные. Столбовыми называются линии, несущими конструкциями являются деревянные или железобетонные опоры. Опорами столбовых линий служат металлические стойки, установленные, например, на крышах зданий. Для изоляции проводов воздушных линий друг от друга и относительно земли их укрепляют на фарфоровых изоляторах.

Более широко применяются кабельные линии связи. Кабельные линии связи получили доминирующее развитие при организации объектовой, городской и междугородной телефонной связи. Они составляют 65% телефонных линий России. Кабели бывают симметричными и коаксиальными.

Если обе жилы цепи, образованного кабелем, выполнены из проволоки одинакового диаметра, имеют изоляцию одинаковой конструкции и расположены так, что между ними можно провести плоскость симметрии, то кабель называется симметричным. Если же оба проводника цепи выполнены в форме соосных цилиндров, в поперечном сечении имеют форму концентрических окружностей, то такой кабель - коаксиальный.

Симметричные кабели представляют собой проводники (жилы) с нанесенными на них одним или несколькими слоями изолятора из диэлектрических материалов. Несколько жил, объединенных единым изолятором в виде ленты, образуют ленточные кабели или полосковые линии. Известные конструкции симметричных кабелей содержат от 1х2 до 2400х2 жил под общей защитной оболочкой.

В коаксиальном кабеле один проводник концентрически расположен внутри другого проводника, имеющего форму полого цилиндра. Внутренний проводник изолируется от внешнего с помощью различных изоляционных материалов и конструкций. Для изоляции коаксиальных пар кабеля применяется сплошной и пористый полиэтилен, изоляция в виде шайб, в последовательно соединенных баллончиков, напоминающий разрез бамбука и др. Для обеспечения гибкости кабеля внешний проводник выполняется из медной или железной сетки, а для защиты от внешних воздействий он покрывается слоем изолятора (полихлорвинила).

Основными параметрами проводных линий связи являются ширина пропускаемого ими спектра частот и собственное затухания $Z_c = 10\ lgP_{вх} / P_{вых}$, где $P_{вх}$ и $P_{вых}$ - мощность сигнала на входе и выходе цепи соответственно.

Если сопротивление проводников на низких частотах (в диапазоне 0-100 кГц) определяется удельным сопротивлением материала и площадью поперечного сечения проводника, то на более высоких частотах начинается сказываться влияние поверхностного эффекта. Сущность его заключается в том, что переменное магнитное поле, возникающее при протекании по проводнику тока, создает внутри проводника вихревые токи, В результате этого плотность основного тока перераспределяется по сечению проводника (жилы): уменьшается в центре и возрастает на периферии. Глубина проникновения (в мм) тока в медную жилу $\theta=67/\sqrt{\mathbf{f}}$, где f-частота колебаний в Гц. На частоте f=60 кГц глубина проникновения составляет приблизительно 0.3 мм, а на частоте 250 кГц - на порядок ниже, всего около 0.03 мм. Следовательно, ток с этой частотой распространяется по гипотетической тонкой медной трубке с существенно меньшей площадью сечения и, соответственно, большим сопротивлением.

На величину затухания линии влияют также электрические характеристики диэлектрика, наносимого на металлические провода. За счет их удается расширить полосу пропускания линии. При передаче по воздушным линиям со стальными проводами ширина пропускания составляет около 25 кГц, с медными проводами - до 150 кГц, по симметричным кабелям - до 600 кГц, Расширению спектра частот, передаваемых по симметричным цепям, препятствуют возрастающие наводки. Например, удовлетворительным для телефонных линий считается значение переходного затухание порядка 60-70 дБ.

В коаксиальном кабеле электрическое поле замыкается между внутренним и внешним проводниками, поэтому внешнее электрическое поле отсутствует. Кабель не имеет также внешнего магнитного и электромагнитного полей, что и обусловливает его основные преимущества перед симметричными. Вследствие поверхностного эффекта ток при повышении частоты оттесняется во внутреннем проводнике к его наружной поверхности, а во внешнем, наоборот, к внутренней. Стандартная коаксиальная пара 1.2/4.4 (с диаметрами внутреннего и внешнего проводников - 1.2 и 4.4. мм соответственно) обеспечивают передачу 900-960 телефонных каналов на расстояние до 9 км или 3600 каналов на расстояние 1.5км. При увеличении диаметров проводников до 2.6/9/5 число телефонных каналов для длины участка 1.5 км возрастает до 10800.Ширина частотного диапазона такого кабеля достигает 60 МГц. Повышение частотного диапазона потребует

дальнейшего увеличения диаметров проводников коаксиального кабеля.

Электромагнитная волна представляет форму существования электромагнитного поля в виде изменяющихся во времени по синусоидальному закону значений напряженности электрического и магнитного полей.

Электромагнитная волна как носитель информации в радиоэлектронном канале утечки возникает при протекании по проводам электрического тока переменной частоты и распространяются от источника ненаправленного излучения радиально во все стороны с конечной скоростью, в атмосфере несколько меньшей скорости света. Векторы напряженности электрического и магнитного полей взаимноперпендикулярны и перпендикулярны направлению распространения электромагнитной волны. Электромагнитная волна характеризуется частотой колебания, мощностью и поляризацией. По частоте электромагнитные волны классифицируются в соответствии с Регламентом радиосвязи, утвержденным на Всемирной административной конференции в Женеве в 1979 г. (табл. 4.3).

Таблица 4.3.

Диапазон длин волн	Наименование волн	Обозначение и наименование частот	Диапазон частот
> 100 км	-	ELF-чрезвычайно низкие	Доли Гц-3 кГц
10-100 км	Мириаметровые	VLF(ОНЧ)-очень низкие	3-30 кГц
1-10 км	Километровые (длинные)	LF(НЧ)-низкие	30-300 кГц
100-1000 м	Гектаметровые (средние)	MF(СЧ)-средние	300-3000 кГц
10-100 м	Декаметровые (короткие)	HF(ВЧ)-высокие	3-30 МГц
1-10 м	Метровые	(ОВЧ)-очень высокие	30-300 МГц
10-100 см	Дециметровые	UHF(УВЧ)-ультравысокие	300-3000 МГц
1-10 см	Сантиметровые	SHF(СВЧ)-сверхвысокие	3-30 ГГц
1-10 мм	Миллиметровые	EHF(КВЧ)-крайне высокие	30-300 ГГц
0.1-1 мм	Децимиллиметровые	ГВЧ-гипервысокие	300-3000 ГГц

Поляризация определяет направление вектора напряженности электрического поля. Если вектор электрического поля лежит в вертикальной плоскости, то поляризация вертикальная, когда он находится в горизонтальной плоскости, то - горизонтальная. Промежуточное положение характеризуется углом поляризации между плоскостями поляризации и распространения. Плоскостью поляризации называется плоскость, в которой находятся вектора электрического поля и вектор распространения электромагнитной волны. Плоскость распространения имеет вертикальное расположение и проходит через вектор распространения электромагнитной волны.

Мощность излучения электромагнитного поля тем выше, чем ближе частота колебаний в распределенном контуре, образованного индуктивностью проводников и распределенной емкостью между ними и землей, к частоте сигнала. Устройства, в которых обеспечивается эффективное преобразование энергии электрических сигналов в электромагнитную волну, называются антеннами.

Антенные устройства являются неотъемлемой частью передающих и приемных радиоэлектронных средств. Причем их конструкция остается неизменными в режимах передачи и приема, за исключением тех случаях, когда излучается большая мощность. В этом случае приходится принимать дополнительные меры по предотвращению электрического пробоя в высоковольтных цепях передающей антенны, необходимость в которых отсутствует для приемной. В общем случае принцип обратимости позволяет передающую антенну использовать в качестве приемной и наоборот.

Характер поляризации электромагнитной волны зависит от конструкции и расположения излучающих элементов антенны. Несоответствие поляризации

электромагнитной волны пространственной ориентации элементов приемной антенны, в которых наводятся электрические заряды, приводит к уменьшению величины этих зарядов. Радиоволны в зависимости от условий распространения делятся на земные (поверхностные), прямые, тропосферные и ионосферные (пространственные).

Земными называются радиоволны, которые распространяются в непосредственной близости от поверхности Земли и частично огибают ее поверхность благодаря явлению дифракции. Прямыми названы радиоволны, распространяющиеся прямолинейно в атмосфере и космосе.

Радиоволны, которые распространяются в тропосфере - приземной неоднородной области атмосферы не выше 10-12 км от поверхности Земли, называются тропосферными. В тропосфере происходит рассеивание, а также частичное искривление траектории и отражение радиоволн от неоднородностей тропосферы. Ионосферными называют радиоволны, распространяющиеся в результате последовательного отражения от ионосферы и земной поверхности. Ионосферу образуют ионизированные под действием ультрафиолетового излучения Солнца верхние слои атмосферы. Концентрация свободных электронов в ионосфере меняется по высоте. В зависимости от концентрации свободных электронов и соответственно положительно заряженных ионов ионосферу условно делят на слои - D, E, F_1 и F_2. Наименьшая концентрация имеет место в слое D, наибольшая - в слое F_2. Состояние ионосферы непрырывно меняется, оно зависит от времени суток, времени года и солнечной активности, которая имеет 11-летний цикл изменения.

Слой D располагается до высоты примерно 60 км. В ночные часы слой D преобладает рекомбинация электронов и ионизация уменьшается или исчезает.

Слой E расположен на высоте 100-120 км и менее зависит от времени суток.

Слои F_1 и F_2 занимают области на высоте примерно 160-400 км, причем ночью слой F_1 исчезает.

В ионосфере происходит преломление, отражение и поглощение радиоволн. Преломление радиоволн обусловлено изменениями диэлектрической проницаемости, а, следовательно, показателя преломления по высоте слоев. По мере распространения радиоволн от наземного источника через более высоко расположенные слои показатель преломления уменьшается, траектория электромагнитной волны искривляется и при определенных условиях волна возвращается на Землю.

Отражение радиоволн на той или иной высоте ионосферы зависит от частоты радиоволн и угла их падения на слой. При прочих равных условиях чем больше угол падения волны, отсчитываемый от вертикальной линии в точке падения, тем более полога траектория луча в ионосфере и тем меньшая электронная концентрация потребуется для возвращения луча на Землю. Минимальное значение угла падения, при котором еще возможно отражение радиоволн от ионосферы называется критическим. При угле падения, меньшем критического, радиоволны проходят через ионосферу не отразившись.

Так как коэффициент преломления уменьшается с увеличением частоты, то длинные волны преломляются сильнее, чем короткие, а для УКВ преломление недостаточно для возвращения волн на Землю и они уходят в космическое пространство. Наивысшая частота, при которой электромагнитная волна еще может возвратиться на Землю, называется максимально применимой частотой. Но значение этой частоты неоднозначно вследствие зависимости ее от угла падения. Поэтому вводят понятие критической частоты, которая является максимально применимой частотой при угле падения 90 градусов. Из определения следует, что эта частота представляет собой низшую из всех максимально применимых частот.

За счет многократного переотражения радиоволн от слоев ионосферы и земной поверхности электромагнитная волна может распространяться на большие расстояния вплоть до огибания Земли. Но при переотражениях возникают зоны молчания, куда не попадают отраженные от ионосферы электромагнитные лучи. В зонах приема происходит

интерференция волн, прошедших разный путь от излучателя и имеющих, следовательно, различные фазы. Случайный характер изменения фаз приводит к случайному изменению амплитуды результирующей волны, которое называется замиранием или федингом.

Степень поглощения радиоволн в атмосфере увеличивается при повышении плотности ионизации, частоты колебания и пути, проходимой радиоволной в ионосфере. Зимой, когда концентрация электронов в связи с понижением солнечной радиации уменьшается, поглощение радиоволн снижается и дальность распространения увеличивается. В зависимости от частоты колебания радиоволн характеристики среды распространения имеют следующие особенности.

1. Километровые (длинные) волны обладают хорошей дифракцией, сравнительно слабо поглощаются земной поверхностью и могут распространяться поверхностным лучом на расстояние до 3000 км. В ионосфере они затухают сильнее, но могут отражаться от слоя Е и распространяться пространственным лучом на большее расстояние. К преимуществам электромагнитной волны в этом диапазоне как носителя информации относится, кроме большой дальности распространения, сравнительное постоянство напряженности поля в пункте приема в течение суток и года, что обеспечивает устойчивость связи. Эти волны применяются также для связи под водой, где плохо распространяются волны более высоких частот.

Недостатком длинноволновой радиолинии является плохая излучательная способность антенн, их большие размеры, достигающие несколько сотен метров, высокий уровень атмосферных и промышленных помех и малая пропускная способность.

2. Гектометровые (средние) волны могут распространяться поверхностным и пространственным лучами. Энергия средних волн поглощаются земной поверхностью сильнее, чем энергия длинноволновых, поэтому дальность связи поверхностным лучем составляет примерно 500 - 1500 км. Однако для средних волн создаются более благоприятные условия распространения пространственным лучом и прием сигналов возможен до 4000 км.

Условия распространения средних волн существенно изменяются в зависимости от времени суток. В ночные часы за счет отражения от ионосферы дальность распространения выше, чем в дневные, когда преобладают поверхностные волны. В этом диапазоне наблюдаются замирания в результате интерференции земных и поверхностных волн или пространственных волн с различными путями распространения, высокий уровень атмосферных и промышленных помех. Антенны в среднем диапазоне по устройству в основном такие же, как и антенны в длинноволновом, но в силу большей близости их геометрических размеров к длинам волн имеют больший коэффициент усиления. Радиоволны в этом диапазоне используются для радиовещания и связи, на флоте и в авиации.

3. При распространении коротких волн дальность поверхностного луча невелика из-за резкого возрастания поглощения энергии в Земле. Поле в точке приема создается в основном за счет отражения от различных слоев ионосферы. В результате флюктуации плотности и высоты слоев и взаимодействия лучей на коротких волнах, как правило, наблюдаются глубокие замирания и даже полное пропадание связи в течение нескольких десятков секунд.

Для обеспечения круглосуточной связи в условиях суточного изменения ионосферы необходимо производить периодическую смену частот. Определение оптимальных частот производится специальными службами наблюдения за ионосферой по результатам вертикального и вертикально-наклонного зондирования ее радиоимпульсами. Наиболее благоприятные условия прохождения волн днем чаще складываются на волнах в интервале 10-25 м, а ночью - 35-70 м.

В диапазоне коротких волн на напряженность поля и характер ее изменения в точке приема влияют другие явления, такие как «вспышки» на Солнце, рассеяние волн на мелких неоднородностях ионосферы, повороте плоскости поляризации.

Достоинством коротких волн является возможность обеспечения связи на очень большие расстояния при сравнительно малых мощности передатчика и габаритах антенны, а также малое влияние атмосферных и промышленных помех. Они применяются для связи, радионавигации, радиовещании и радиолюбителями.

4. В диапазоне ультракоротких (метровых) и более коротких волн практически отсутствует дифракция. Поэтому они распространяются в пределах прямой видимости, в том числе отражаясь от земли и тропосферы с потерей части энергии на поглощение. Радиоволны в этих диапазонах являются основными носителями информации в сетях телекоммуникаций человечества в силу следующих особенностей:

- имеют огромный частотный диапазон (см. табл. 4.3), обеспечивающий возможность передачи огромного объема информации, в том числе путем использования широкополосных каналов;
- низкий уровень атмосферных и промышленных помех, позволяющих использовать приемные устройства с высокой чувствительностью, что повышает дальность приема;
- слабое влияние станционных помех на работу других радиосистем вследствие ограниченности их радиуса видимости;
- возможность создания небольших антенн с узкой диаграммой направленности, позволяющих осуществлять радиосвязь при относительно малой мощности передающих устройств. Основным недостатком радиоволн рассматриваемого диапазона - малая дальность распространения и существенно большее поглощение их природными осадками (дождем, туманом, снегом, градом), особенно в миллиметровом и более коротких диапазонах.

Результаты сравнительного анализа характеристик радиоволн различных диапазонов приведены в табл. 4.4.

Таблица 4.4.

Диапазон	Дальность распространения	Антенны	Уровень помех	Поглощение в атмосфере
ДВ	Поверхностной волной - до 3 тыс. км, пространственной - до 20 тыс. км	Громоздкие	Высокий	Слабое
СВ	Поверхностной - до 1500 км			
КВ	Пространственной - - на любое расстояние			
УКВ	Прямая видимость	Компактные	Низкий	Сильное

Для повышения дальности связи применяют следующие методы:

- подъем передающей или приемной антенн с помощью инженерных конструкций (матч, башен) и летно-подъемных аппаратов (аэростатов);
- ретрансляция радиосигналов с помощью наземных и космических ретрансляторов;
- использование тропосферных волн в УКВ диапазоне.

Передающие антенны на башнях устанавливаются для постоянного обеспечения связи, радио и телевизионного вещания в городах, районах и областях. Для периодического и эпизодического приема сигналов от отдаленных источников в качестве носителей приемников сигналов используют привязные аэростаты. Информация с них на землю передается по кабелю или радиоканалу.

Для передачи информации в УКВ и СВЧ диапазонах частот на большие расстояния широко применяются ретрансляторы. С помощью наземных ретрансляторов создаются радиорелейные линии (РРЛ), представляющие собой цепочку приемопередающих станций, каждая из которых устанавливается в пределах прямой видимости соседних. Все

станции РРЛ разделяются на оконечные, промежуточные и узловые. Оконечные радиорелейные станции располагаются в начале и конце линии. На этих станциях вводится и выделяется информация, обеспечивается распределение информации между потребителями. Промежуточные станции предназначены для ретрансляции сигналов. Узловые радиорелейные станции - это промежуточные станции, на которых происходит разветвление принимаемых сигналов по различным направлениям, выделение части принимаемых передаваемой информации (например, программы телевидения) и введение новой информации.

Диапазон частот, предназначенных для передачи информации одного вида, объединяются в радиочастотный ствол: телевизионный, телефонный и т. д. Существующие отечественные РРЛ могут содержать до 8 стволов, а ствол, например, телефонный - до 1920 телефонных каналов. Для каждого ствола с целью исключения взаимного влияния выделяются две рабочие частоты - для передачи и приема. Принятые каждой станцией сигналы на частоте приема усиливаются и преобразуются на частоте передачи и излучаются в направлении следующей станции. Около 30% телефонных каналов РФ обеспечивает радиорелейная связь.

Разновидностью радиорелейных линий связи являются тропосферные линии связи, использующие явление рассеяние ультракоротких радиоволн в неоднородностях тропосферы. К таким неоднородностям относятся области тропосферы с резко изменившимися значениями диэлектрической проницаемости. Неоднородности вызываются неравномерностью состояний различных точек тропосферы, непрерывным перемешиванием и смещением воздушных масс в результате неравномерного разогрева Солнцем различных участков поверхности Земли и слоев тропосферы. Для устойчивой тропосферной радиосвязи применяют антенны с высоким коэффициентом усиления (40-50 дБ), мощные передатчики (1-10 кВт) и высокочувствительные приемники. Тропосферные линий связи чаще всего имеют протяженность 140-500 км.

Ретрансляторы, устанавливаемые на искусственных спутниках Земли (ИСЗ), наиболее широко используются для обмена информацией между абонентами, удаленных друг от друга на тысячи километров. Они является элементами (звеньями) спутниковых линий связи, которые содержат также оконечные наземные передающие и приемные станции. Естественно, что связь возможно лишь в том случае, если спутники находятся в зоне видимости обеих земных станций.

Для ретрансляции применяются в основном ИСЗ на геостационарной (стационарной) и эллиптической орбитах, а также менее дорогие низкоорбитальные КА.

При распространении радиоволн в городе характер их распространения существенно искажается по сравнению с распространением на открытых пространствах за счет многочисленных переотражений от стен зданий и помещений и затухания в их них. Эти обстоятельства необходимо учитывать при оценке пространственной ориентации и возможностей каналов утечки информации. Экранирующие свойства некоторых элементов здания приведены в табл. 4.5.

Таблица 4.5.

Тип здания	Ослабление, дБ на частоте		
	100 МГц	500 МГц	1 ГГц
Деревянное здание с толщиной стен 20 см	5-7	7-9	9-11
Кирпичное здание с толщиной стен 1.5 кирпича	13-15	5-17	16-19
Железобетонное здание с ячейкой арматуры 15х15 см и толщиной 160 мм	20-25	18-19	15-17

Указанные в таблице данные получены для стен, 30 процентов площади которых занимают оконные проемы с обычным стеклом. Если оконные проемы закрыты металлической решеткой с ячейкой 5 см, то экранирование увеличивается на 30-40 %.

Дальность распространения электромагнитной волны из здания с толстой кирпичной

или железобетонной стенами уменьшается по отношению к экранированию стен деревянного здания в 2-3 раза в зависимости от частотного диапазона.

Многообразие природных и искусственных источников излучений в радиодиапазоне порождает проблему электромагнитной совместимости носителя информации с другими излучениями-носителями иной информации, которые представляют собой помехи по отношению к рассматриваемому радиосигналу. Классификация помех представлена на рис. 4.5.

Рис. 4.5. Классификация помех в каналах утечки.

Природные или естественные помехи вызываются следующими природными явлениями:

- электрическими грозовыми разрядами, как правило, на частотах менее 30 Мгц;
- перемещением электрически заряженных частиц облаков, дождя, снега и др.,
- возникновением резонансных электрических колебаний между землей и ионосферой;
- тепловым излучением Земли и зданий в диапазоне более 30-40 МГц;
- солнечной активностью в основном на частотах более 20 МГц;
- электромагнитными излучениями неба, Луны, других планет (на частотах более 1 МГц);
- тепловыми шумами в элементах радиоприемниках.

В городах к естественным помехам добавляются промышленные помехи, которые по характеру спектра излучений делятся на флюктуационные, гармонические и импульсные.

Флюктуационные помехи имеют распределенный по частоте спектр и создаются коронами высоковольтных электропередач, лампами дневного света, неоновой рекламой, электросваркой и другими электрическими процессами. Спектр промышленных гармонических помех локализован на частотах излучений, возникающих при нелинейных преобразованиях в промышленных установках. Импульсные помехи, возникающие, прежде всего, при замыкании и размыкании электрических контактов выключателей, характеризуются сосредоточением энергии электромагнитных излучений в короткий промежуток времени.

Так как электромагнитные волны в радиодиапазоне являются основными носителями информации, то с целью нарушения управления и связи в ходе радиоэлектронной борьбы созданы разнообразные средства генерирования помех.

По эффекту воздействия радиоэлектронные помехи делятся на маскирующие и имитирующие. Маскирующие помехи создают помеховый фон, на котором затрудняется или исключается обнаружение и распознавание полезных сигналов. Имитирующие помехи по структуре близки к полезным сигналам и при приеме могут ввести в заблуждение получателя.

По соотношению спектра помех и полезных сигналов помехи подразделяются на заградительные и прицельные. Заградительные помехи имеют ширину спектра частот, значительно превышающую ширину спектра полезного сигнала, что позволяет подавлять сигнал без точной настройки на его частоту. Прицельная помеха имеет ширину спектра, соизмеримую (равную или превышающую в 1.5-2 раза) с шириной спектра сигнала, и создает высокий уровень спектральной плотности мощности в полосе частот сигнала при невысокой средней мощности передатчика помех.

По временной структуре излучения помехи бывают непрерывные и импульсные (в виде немодулированных или модулированных радиоимпульсов).

4.5. Акустические каналы утечки информации

В акустическом канале утечки носителем информации от источника к несанкционированному получателю является акустическая волна в атмосфере, воде и твердой среде. Источниками ее могут быть:

- говорящий человек, речь которого подслушивается в реальном масштабе времени или озвучивается звуковоспроизводящим устройством;
- механические узлы механизмов и машин, которые при работе издают акустические волны.

Структура этого канала утечки информации принципиально не отличается от структуры рассмотренных каналов утечки информации и приведена на рис 4.6.

Рис. 4.6. Структура акустического канала утечки информации.

Источниками акустического сигнала могут быть люди, звучащие механические, электрические или электронные устройства, приборы и средства, воспроизводящие ранее записанные звуки. Источники сигналов характеризуются диапазоном частот, мощностью излучения в Вт, интенсивностью излучения в Вт/м^2 - мощностью акустической волны, прошедшей через перпендикулярную поверхность площадью 1 м^2 , громкостью звука в дБ, измеряемой как десятичный логарифм отношения интенсивности звука к интенсивности звука порога слышимости. Порог слышимости соответствует мощности звука 10^{-12} Вт или звуковому давлению на барабанную перепонку уха человека $2 \cdot 10^{-5}$ Па. Уровни громкости различных звуков иллюстрируются данными табл. 4.6.

Таблица 4.6

Оценка громкости звука на слух	Уровень звука, дБ	Источник звука
Очень тихий	0	Усредненный порог чувствительности уха
	10	Тихий шепот (1.5 м)
Тихий	20	Тиканье настенных механических часов
	30	Шаги по мягкому ковру (3-4 м)
	40	Тихий разговор, шум в читальном зале
Умеренный	50	Шум в жилом помещении, легковой автомобиль (10-15 м)
	60	Улица средней шумности
Громкий	70	Спокойный разговор (1 м), зал большого магазина
	80	Радиоприемник громко (2 м), крик
Очень громкий	90	Шумная улица, гудок автомобиля
	100	Симфонический оркестр, автомобильная сирена
Оглушительный	110	Пневномолот, очень шумный цех
	120	Гром над головой
	130	Звук воспринимается как боль

Среда распространения носителя информации от источника к приемнику может

быть однородной (воздух, вода) и неоднородной, образованной последовательными участками различных физических сред: воздуха, древесины дверей, стекол окон, бетона или кирпича стен, различными породами земной поверхности и т. д. Но и в однородной среде ее параметры не постоянные, а могут существенно отличаться в разных точках пространства.

Акустические волны как носители информации характеризуются следующими показателями и свойствами:

- скоростью распространения носителя;
- величиной (коэффициентом) затухания или поглощения;
- условиями распространения акустической волны (коэффициентом отражения от границ различных сред, дифракцией).

Теоретически скорость звука определяется формулой Лапласа:

$$C_{зв} = \sqrt{\mathbf{K} / \rho},$$

где К-модуль всесторонней упругости (когда сжатие производится без притока и отдачи тепла) вещества среды распространения;

ρ-плотность вещества среды распространения.

Для газов модуль всесторонней упругости равен их давлению. При сжатии газа увеличение давления сопровождается пропорциональным увеличением его плотности. Поэтому скорость звука в газе не зависит от его плотности, а пропорциональна корню квадратному из температуры газа, значению универсальной газовой постоянной, отношению величин теплоемкостей газа при постоянном объеме и давлении.

Скорость звука в морской воде зависит от трех основных параметров: температуры t, солености s и давления, которое определяется глубиной h. Для определения скорости звука в морской воде используется формула Лероя, которая имеет вид:

$$v = 1492.2 + 3(t - 10) - 6x10^{-3}(t - 10)^2 - 4x10^{-2}(t - 18)^2 + 1.2(s - 35) - 10^2 (t - 18)(s - 35) + h/61,$$

где v выражено в м/с, t - в градусах Цельсия, s - в промилях, h - в метрах.

Скорость распространения звука в твердых телах определяется в основном их плотностью и упругостью.

Значение скорости распространения звука в некоторых типичных средах приведены в табл. 4.7.

Таблица 4.7.

Среда распространения	Скорость, м/с
Воздух при температуре:	
0^o С	332
$+20^o$ С	344
Вода морская	1440-1540
Железо	5170
Стекло	3500-5300
Дерево	4000-5000
Горные породы	5000-8000

При распространении звуковых колебаний движение частиц среды вызывает давление во фронте волны. Фронтом звуковой волны называется поверхность, соединяющей точки поля с одинаковой фазой колебания. По мере распространения в любой среде звуковые волны затухают. Затухание звуковых волн в морской воде больше, чем в дистиллированной и меньше (почти в 1000 раз), чем в воздухе. При этом величина затухания зависит от длины акустической волны. С увеличением частоты величина затухания быстро возрастает, поэтому при постоянной мощности излучения дальность распространения с ростом частоты падает.

При распространении акустической волны в среде ее траектория изменяется в результате отражений и дифракции. На границе сред с разной плотностью акустическая волна частично переходит из одной среды в другую, частично отражается от границы

между двумя средами. Доля проникшего или отраженного звука зависит от соотношения значений акустических сопротивлений сред, равных произведению удельной плотности вещества β на скорость звука в нем v. Коэффициент проникновения звука *c* (в иную среду при существенном различии акустических сопротивлений сред оценивается по приближенной формуле Рэлея: $\beta \approx 4cv_1\beta_{1/}\ v_2\beta_2$. В соответствии с ней при нормальном падении звука из воздуха на воду, бетон, дерево в эти среды проникает не более тысячной доли интенсивности звука. Отражение звука может происходить от поверхности раздела слоев воздуха и воды с разными значениями акустического сопротивления вследствие неодинаковой температуры и плотности. Этим объясняется значительные колебания (в 10 и более раз) дальности распространения звука в атмосфере. Заметное влияние на характер распространения акустической волны в атмосфере может оказать ветер. При определенных условиях неоднородности создают условия для образования акустических (звуковых) каналов, по которым акустическая волна может распространяться на значительно большие расстояния, как свет по оптическим светопроводам. Акустические каналы чаще всего образуются в воде морей и океанов на определенной глубине, на которой в результате влияния двух противоположных природных факторов (плотности воды и ее температуры) минимизируется скорость распространения акустической волны. Скорость распространения акустической волны в воде, с одной стороны, увеличивается с глубиной из-за повышения плотности воды, но, с другой стороны, уменьшается при понижении ее температуры в более глубоких слоях, особенно в летнее время. В результате этих двух противоположных факторов влияния на определенной глубине, зависящей от температуры над поверхностью воды и ее солености, образуются области с минимумом скорости распространения акустической волны. Акустическая волна, попадающая в эту область, распространяется внутри ее с соответствующим для параметров воды затуханием. При отклонении траектории распространения волна, преломляясь в неоднородностях области, возвращается в канал. В акустическом канале звуковая волна от подводных взрывов может распространяться на расстояние в сотни и тысячи км.

При каждом отражении часть энергии звука теряется вследствие поглощения. Отношение поглощенной энергии звука к падающей называется коэффициентом поглощения . Коэффициенты поглощения звука α некоторых материалов приведены в табл. 4.8.

Таблица 4.8.

Материалы	α	Материалы	α
Оштукатуренная кирпичная стена	0.025	Линолеум	0.12
Бетонная стена	0.015	Ковер	0.20
Стекло	0.027	Паркет	0.06

За счет многократных переотражений акустической волны в замкнутой среде распространения возникает явление послезвучания - реверберация. Величина реверберации оценивается временем T_p после выключения источника звука, в течение которого энергия звука уменьшается на 60 дБ. Вследствие многократных переотражений на мембрану микрофона в помещении оказывают давление акустические волны, распространяющиеся разными путями от источника звука. Интерференция волн с разными фазами могут при достаточно большом времени реверберации приводить к ухудшению соотношения сигнал/помеха в точке приема и уменьшению разборчивости речи. Чем больше размеры помещения и меньше коэффициент поглощения ограждающих поверхностей, тем больше время реверберации. При большом времени реверберации помещение кажется гулким. Однако при очень малом T_p на микрофон воздействует, в основном, быстрозатухающая прямая волна, слышимость речи при удалении от источника резко уменьшается, тембр звуков речи за счет большего затухания в среде распространения высоких частот обедняется. Время реверберации менее 0.85 с незаметно

для слуха. Для большинства помещений организаций их объемы и акустическая отделка время реверберации мало (0.2-0.6) с и его можно не учитывать при оценке разборчивости.

Для концертных залов, имеющих существенно большие размеры, время реверберации определяет их акустику. Установлено, что в малых помещениях объемом V до 350 м^2 оптимальной является реверберация со временем до 1.06 сек. При увеличении объема помещения время реверберации пропорционально повышается и принимает для V=27000 м^3 значение около 2 сек.

Время реверберации в помещении объемом V вычисляется по формуле Эйринга:

$$T_p = - 0.07V/Slg(1-\alpha_{ch}),$$

где S - суммарная площадь всех поверхностей помещения;

$\alpha_{ср} = \sum_{\forall i} \alpha_к S_к$ - средний коэффициент звукопоглощения в помещении;

$S_к$ и $\alpha_к$ - площади и коэффициенты поглощения ограждающих поверхностей соответственно.

При распространении структурного звука в конструкциях зданий, особенно, в трубопроводах возникают реверберационные искажения, снижающие разборчивость речи на 15-20%.

Акустическая волна в отличие от электромагнитной в значительно большей степени поглощается и в среде распространения. Поэтому дальность акустического канала утечки информации, в особенности от такого маломощного источника как человек, мала и, как правило, не обеспечивает возможность ее съема за пределами территории предприятия. Речь человека при обычной громкости может быть непосредственно подслушана злоумышленником на удалении единиц и в редких случаях - десятков метров, что, естественно, крайне мало.

Ухудщение разборчивости речи при прохождении звука через различнык строительные конструкции люстрируются данными в табл. 4.9.

Таблица 4.9.

Тип конструкции	Ожидаемая разборчивость слогов, %
Кирпичная стена (1 кирпич)	25/0
Гипсолитовая стена	90/0
Деревянная стена	99/63
Пластиковая стена	99/55
Дверь обычная филенчатая	100/73
Дверь двойная	95/36
Окно с одним стеклом 3 мм	90/33
Окно с одним стеклом 6 мм	87/15
Оконный блок 2х3 мм	82/0
Вентиляционный канал 20 м	90/2
Оконный кондиционер	95/63
Бетонная стена	88/0
Перегородка внутренняя	96/80
Трубопровод (в соседнем помещении)	95/55
Трубопровод (через этаж)	87/36

Примечание: в числителе указаны значения разборчивости речи при малом уровне акустических шумов, в знаменателе - при сильном.

Акустические шумы и помехи вызываются многочисленными источниками - автомобильным транспортом, ветром, техническими средствами в помещениях, разговорами в помещениях и т. п. Уровни шумов изменяются в течение суток, дней недели, зависят от погодных условий. Ночью и в выходные дни помехи меньше. Средние значения акустических шумов на улице составляют 60-75 дБ в зависимости от

интенсивности движения автомашин в районе расположения здания. Уровень шумов в помещениях по существующим нормам не должен превышать 50 дБ. В трубопроводах отопления помехи изменяются от 10-15 дБ в отсутствие воды и 15-20 дБ при ее наличии.

При утечке акустической информации через вентиляционные воздухопроводы они ослабевают из-за изменения их сечения, поглощений в изгибах. Затухание в прямых металлических воздуховодах составляет 0.15 дБ/м, в неметаллических - 0.2-0.3 дБ/м. При изгибах затухание достигает 3-7 дБ (на один изгиб), при изменениях сечения - 1-3 дБ. Ослабление сигнала на выходе из воздуховода помещения составляет 10-16 дБ.

Поиски путей повышения дальности добывания речевой информации привели к появлению составных каналов утечки информации. Применяются два вида составного канала утечки информации: акусто-радиоэлектронной и акусто-оптический.

Акусто-радиоэлектронный канал утечки информации состоит из двух последовательно сопряженных каналов: акустического и радиоэлектронного каналов утечки информации. Приемником акустического канала является функциональный или случайно образованный акустоэлектрический преобразователь. Электрический сигнал с его выхода поступает на вход радиоэлектронного канала утечки информации - источника электрических или радиосигналов.

Структура акусто-радиоэлектронного канала утечки информации приведена на рис. 4.7.

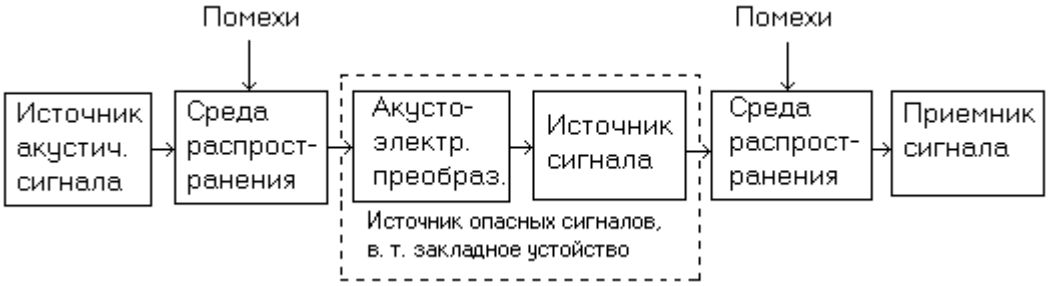


Рис. 4.7. Структура акусто-радиоэлектронного канала утечки информации.

Пара “акустоэлектрический преобразователь-источник сигнала” образуют источник опасных сигналов или реализуются в закладном устройстве, размещаемом злоумышленником в помещении с конфиденциальной информацией. Закладные устройства создаются специально для подслушивания речевой информации и обеспечивают повышения дальности составного акустического канала до единиц км и возможность съема информации злоумышленником за пределами контролируемой зоны.

Закладное устройство как ретранслятор является более надежным элементом канала утечки, чем источник опасного сигнала, так как процесс образования канала утечки информации на основе закладки управляем злоумышленником.

Другой способ повышения дальности акустического канала утечки информации реализуется путем создания составного акусто-оптического канала утечки информации. Схема его указана на рис. 4.8.

Рим. 4.8. Структурная схема акусто-оптического канала утечки информации,

Составной акусто-оптический канал утечки информации образуется путем съема информации с плоской поверхности, колеблющейся под действием акустической волны с информацией, лазерным лучем в ИК-диапазоне. В качестве такой поверхности

используется внешнее стекло закрытого окна в помещении, в которой циркулирует секретная (конфиденциальная) информация. Теоретически рассматривается возможность съема информации с внешней стороны стены помещения, но данных о реализации подобной идеи нет.

С целью образования оптического канала стекло облучается лазерным лучем с внешней стороны, например, из окна противоположного дома. Луч лазера в ИК-диапазоне для посторонних лиц и находящихся в помещении невидим. В месте соприкосновения лазерного луча со стеклом происходит акустооптическое преобразование, т. е. модуляция лазерного луча акустическими сигналами от разговаривающихся в помещении людей.

Модулированный лазерный луч принимается оптическим приемником аппаратуры лазерного подслушивания, преобразуется в электрический сигнал, усиливается, фильтруется, демодулируется и подается в головные телефоны для прослушивания оператором или в аудимагнитофон для консервации.

4.6. Материально-вещественные каналы утечки информации

Особенность этого канала вызвана спецификой источников и носителей информации сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты (макро и микрочастицы), которые имеют четкие пространственные границы локализации, за исключением (-излучений радиоактивных веществ. Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Для более четкого описания рассматриваемого канала целесообразно уточнить состав источников и носителей информации.

Основными источниками материально-вещественного канала утечки информации являются следующие:

- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся на предприятии (организации);
- отходы делопроизводства и издательской деятельности на предприятии (организации), в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;
- нечитаемые дискеты ПЭВМ из-за их физических дефектов и искажений загрузочных или других кодов;
- бракованная продукция и ее элементы;
- отходы производства в газообразном, жидком и твердом виде.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами:

- сотрудниками организации и предприятия;
- воздушными массами атмосферы;
- жидкой средой;
- излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках - в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т. д.; демаскирующие - в газообразных, жидких и твердых отходах производства.

Структура материально-вещественного канала утечки информации приведена на рис. 4.9.

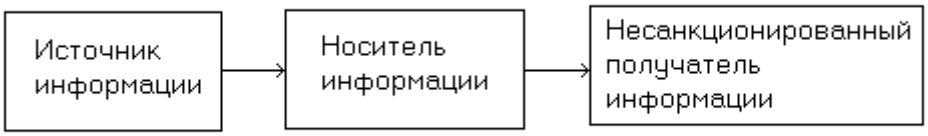


Рис. 4.9. Структура материально-вещественного канала утечки информации.

Приемники информации этого канала достаточно разнообразны. Это эксперты зарубежной разведки или конкурента, средства для физического и химического анализа, средства вычислительной техники, приемники радиоактивных излучений и др.

Потери носителей с ценной информацией возможны при отсутствии на предприятии четкой системы учета носителей с закрытой информацией. Например, испорченный машинисткой лист отчета может быть выброшен ею в корзину для бумаги, из которой он будет уборщицей перенесен в бак для мусора на территории предприятия, а далее при перегрузке бака или транспортировки мусора на свалку лист может быть унесен ветром и поднят прохожим. Конечно, вероятность обеспечения случайного контакта с этим листом злоумышленника невелика, но если последний активно занимается добыванием информации, то область пространства, в котором возможен контакт, значительно сужается и вероятность утечки повышается.

Для предприятий химической, парфюмерной, фармацевтической и других сфер разработки и производства продукции, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ (материалов), возможно образование каналов утечки информации через выбросы в атмосферу газообразных или слив в водоемы жидких демаскирующих веществ.

Подобные каналы образуются при появлении возможности добывания демаскирующих веществ в результате взятия злоумышленниками проб воздуха, воды, земли, снега, пыли на листьях кустарников и деревьев, на траве и цветах в окрестностях предприятия (организации).

В зависимости от розы (направлений) и скорости ветра демаскирующие вещества в газообразном виде или в виде взвешенных твердых частиц могут распространяться на расстояние в единицы и десятки км, достаточное для безопасного взятия проб злоумышленниками. Аналогичное положение наблюдается и для жидких отходов.

Конечно, концентрация демаскирующих веществ при удалении от источника убывает, но при утечке их в течение некоторого времени концентрация может превышать допустимые значения за счет накопления демаскирующих веществ в земле, растительности и подводной флоре и фауне.

Отходы могут продаваться другим предприятиям для использования в производстве иной продукции, очищаться перед сливом в водоемы, уничтожаться или подвергаться захоронению на время саморазрушения или распада. Последние операции выполняются для высокотоксичных вещества, утилизация которых другими способами экономически нецелесообразно и для радиоактивных отходов, которые нельзя нейтрализовать физическими или химическими способами.

Утечка информации о радиоактивных веществах возможна в результате выноса радиоактивных веществ сотрудниками предприятия (организации) или регистрации злоумышленником их излучений с помощью соответствующих приборов, рассмотренных в разделе 3.4.

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для α-излучений она составляет в воздухе единицы мм, β-излучений - см, только γ-излучения можно регистрировать на удалении в сотни метров от источника излучения.

4.7. Комплексирование каналов утечки информации

Многообразие рассмотренных каналов утечки информации предоставляет злоумышленнику большой выбор возможностей для добывания информации. Из анализа возможностей каждого из рассмотренных каналов можно сделать следующие выводы.

1. Утечка семантической информации возможна по всем техническим каналам. По возможностям, а, следовательно, по угрозе безопасности информации они ранжируются в следующей последовательности: радиоэлектронный, акустический и оптический каналы. Однако в некоторых конкретных условиях возможны иные ранги каналов, например, когда имеется реальная предпосылка для наблюдения или фотографирования документов.

2. Наибольшими потенциальными возможностями по добыванию информации о видовых демаскирующих признаках обладает оптический канал, в котором информация добывается путем фотографирования. Это обусловлено следующими особенностями фотоизображения:

- имеет самое высокое разрешение; даже на относительно большом расстоянии в сотни км от объекта наблюдения разрешение при космической фотосъемке достигает 15-30 см на местности;
- имеет самую высокую информационную емкость, обусловленную максимумом демаскирующих признаков, в том числе наличием такого информативного признака как цвет;
- обеспечивает относительно низкий уровень геометрических искажений.

Информационные емкости телевизионных изображений примерно на порядок ниже фотоизображений. Телевизионные изображения имеют более низкий уровень разрешения, повышенный уровень яркостных искажений за счет неравномерности спектрально-яркостных характеристик фотокатода передающих телевизионных трубок или приборов с зарядовой связью, повышенный уровень геометрических искажений за счет дополнительных искажений при формировании электронного растра.

Изображения в ИК-диапазоне обладают еще более низкими информационными параметрами. Кроме более низкой разрешающей способности и больших искажений для изображений в ИК-области характерны крайняя изменчивость в течение суток.

Однако, как уже отмечалось при рассмотрении каналов утечки информации, изображение в каждом из них содержит дополнительные признаки за счет различной их природы.

3. Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный. В значительно меньшем объеме утечка информации о сигнальных демаскирующих признаках возможна в акустическом и материально-вещественном каналах.

Для добывания информации злоумышленник, как правило, использует несколько каналов ее утечки. Комплексирование каналов утечки информации основывается на следующих принципах:

- комплексируемые каналы дополняют друг друга по своим возможностям;
- эффективность комлексирования повышается при уменьшении зависимости между источниками информации и демаскирующими признаками в разных каналах.

Комплексирование каналов утечки информации обеспечивает:

- увеличение вероятности обнаружения и распознавания объектов за счет расширения их текущих признаковых структур;
- повышение достоверности семантической информации и точности измерения признаков, в особенности в случае добывания информации из недостаточно надежных источников.

Когда возникают сомнения в достоверности информации, то с целью исключения дезинформации, полученные сведения и данные перепроверяют по другому каналу.

Возможны два основных вида комплексирования каналов утечки информации - обеспечение утечки информации от одного источника по нескольким параллельно

функционирующим канала (см. рис.4.10 а) и от разных источников (рис. 4.10 б).

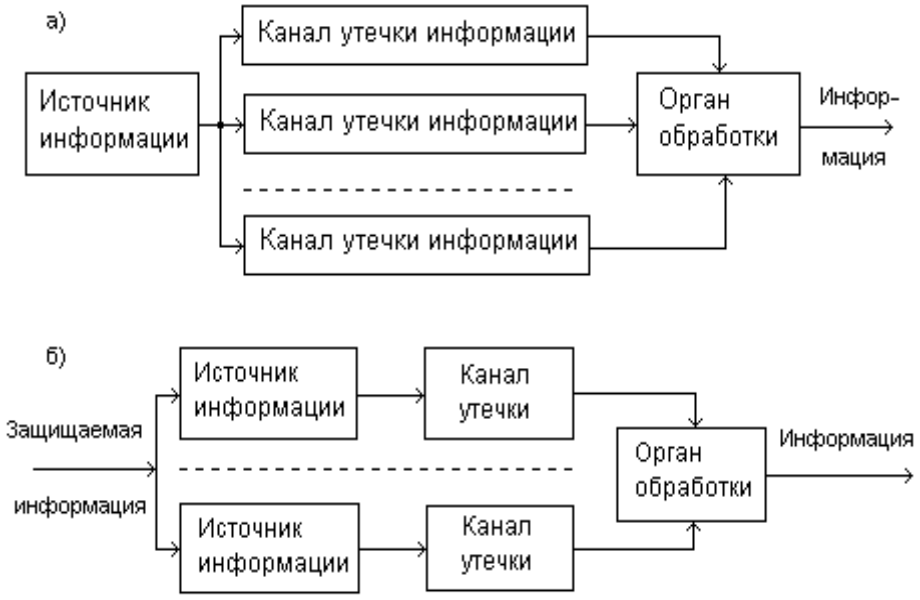


Рис. 4.10. Варианты комплексного использования каналов утечки.

В первом варианте одна и та же информация распространяется по различным направлениям одним или разными носителями. Например, речевая информация разговаривающих в помещении людей может быть подслушана через дверь или стену, снята с опасных сигналов или передана с помощью закладного устройства.

Так как вероятность воздействия помех в разных каналах на одинаковые элементы информации мала, то в этом случае повышается достоверность суммарной информации после обработки ее в соответствующем органе. При независимости помех в n-каналах утечки информации вероятность поражения одного и того же элемента информации при комплексировании n каналов рассчитывается по формуле:

$Pn = \prod_{i=1}^{n} \mathbf{P_i}$, где Pi - вероятность поражения элемента информации в i-ом канале.

Однако если источник не владеет достоверной информацией или занимается дезинформацией, то рассмотренный вариант комплексирования не повышает достоверность итоговой информации. Для обеспечения такой возможности одна и та же информация добывается от нескольких источников, например, из документа и от специалистов, участвующих в создании этой информации. При таком комплексировании 2-х каналов вероятность внедрения дезинформации можно оценить по формуле:

$$Pд = P_1 P_2 + r\sqrt{\mathbf{P_1(1-P_1)P_2(1-P_2)}},$$

где P_1 и P_2 - значения вероятности появления дезинформации в 1-ом и 2-ом каналах;

r - коэффициент корреляции между информацией в этих каналах.

Коэффициент r корреляции характеризует статистическую зависимость между информацией (содержанием или признаками) в каналах. При r =1 по каналам производится утечка информации одинакового содержания или об одинаковых признаках с разными значениями, при r = 0 - источники независимые.

Как следует из этой формулы, для уменьшения риска получения дезинформации необходимо снижать коэффициент корреляции между источниками информации.

Глава 5. Методы инженерной защиты и технической охраны объектов

5.1 Методы защиты информации от утечки по техническим каналам

Защита информации по акустическому каналу

Звукоизоляция помещений

Виброакустическая маскировка

Методы и средства обнаружения и подавления диктофонов диктофонов и акустических закладок

Методы и средства защиты телефонных линий

Методы и средства защиты информации от перехвата компьютерной информации

- Экранирование технических средств
- Заземление технических средств
- Фильтрация информационных сигналов
- Пространственное и линейное зашумление

Методы и средства поиска электронных устройств перехвата информации

5.2 Защита информации по акустическому каналу

Для защиты акустической (речевой) информации используются пассивные и активные методы и средства.

Пассивные методы защиты акустической (речевой) информации направлены на:

- ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- ослабление информационных электрических сигналов в соединительных линиях вспомогательных технических средствах слежения (ВТСС), имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);
- обнаружение излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи;
- обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической (речевой) информации направлены на:

- создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до

величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки;

- создание маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- электромагнитное подавление диктофонов в режиме записи;
- ультразвуковое подавление диктофонов в режиме записи;
- создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- подавление (нарушение функционирования) средств несанкционированного подключения к телефонным линиям;
- уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.

Ослабление акустических (речевых) сигналов осуществляется путем звукоизоляции помещений.

Ослабление информационных электрических сигналов в соединительных линиях ВТСС и исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства осуществляется методами фильтрации сигналов.

В основе активных методов защиты акустической информации лежит использование различного типа генераторов помех, а также применение других специальных технических средств.

5.2.1 Звукоизоляция помещений

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акустической (речевой) информации по прямому акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы водо-, тепло- и газоснабжения, канализации и т.д.) каналам.

Основное требование к звукоизоляции помещений заключается в том, чтобы за его пределами отношение акустический сигнал/шум не превышало некоторого допустимого значения, исключающего выделение речевого сигнала на фоне естественных шумов средством разведки. Поэтому к помещениям, в которых проводятся закрытые мероприятия, предъявляются определенные требования по звукоизоляции.

Звукоизоляция оценивается величиной ослабления акустического сигнала, которое для сплошных однослойных или однородных ограждений (строительных конструкций) на средних частотах приближенно рассчитывается по формуле:

$K_{OГ} \approx 20 \bullet \lg(q_{П} \bullet f) - 47{,}5$, дБ

где $q_{П}$ - масса 1 м^2 ограждения, кг;

f - частота звука, Гц.

Учитывая, что средняя громкость звука говорящего в служебном помещении составляет около 50 ... 60 дБ, то в зависимости от категории помещения его звукоизоляция должна быть не менее норм, приведенных в табл. 5.1.

Таблица 5.1 - Требования к звукоизоляции помещений

Частота, Гц	Категория выделенного помещения, дБ		
	1	2	3
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и его акустических свойств. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны.

Характер этого поглощения определяется соотношением частот падающей акустической волны и спектральных характеристик поверхности средства звукоизоляции.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна.

Двери имеют существенно меньшие по сравнению со стенами и межэтажными перекрытиями поверхностные плотности и трудноуплотняемые зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации (см. табл. 5.2).

Таблица 5.2 - Звукоизоляция обычных дверей

Конструкция двери	Условия применения	Звукоизоляция (дБ) на частотах, Гц					
		25	250	500	1000	2000	4000
Щитовая дверь, облицованная	без прокладки	1	23	24	24	24	23

фанерой с двух сторон	с прокладкой из пористой резины	7	27	32	35	34	35
Типовая дверь П-327	без прокладки	3	23	31	33	34	36
	с прокладкой из пористой резины	9	30	31	33	34	41

Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д.

Как видно из табл. 5.2, применение уплотняющих прокладок повышает звукоизоляцию дверей, однако при этом необходимо учитывать, что в процессе эксплуатации в результате обжатия, износа, затвердевая резиновых прокладок звукоизоляция существенно снижается.

Таблица 5.3 - Звукоизоляция окон

Схема остекления	**Звукоизоляция (дБ) на частотах, Гц**					
	25	**50**	**00**	**000**	**000**	**000**
Одинарное остекление:						
толщина 3 мм	7	7	2	8	1	2
толщина 4 мм	8	3	6	1	2	2
толщина 6 мм	2	2	6	0	7	5
Двойное остекление с воздушным промежутком:						
57 мм (толщина 3 мм)	5	0	2	1	9	6
90 мм (толщина 3 мм)	1	9	8	4	0	8
57 мм (толщина 4 мм)	1	1	8	6	9	5
90 мм (толщина 4 мм)	5	3	1	7	8	6

Для повышения звукоизоляции проводится облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями, а двери обиваются материалами со слоями ваты или войлока и используются дополнительные уплотнительные прокладки.

Звукопоглощающая способность окон, так же как и дверей, зависит, главным образом, от поверхностной плотности стекла и степени прижатия притворов. В табл. 2.4

указаны некоторые данные по звукоизоляции наиболее распространенных вариантов остекления помещений.

Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении. Существенно большую звукоизоляцию имеют окна с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или тройное комбинированное остекление.

Обычные окна с двойными переплетами обладают более высокой (на 4 ... 5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях, когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20 ... 40 мм и с воздушным зазором между стеклами не менее 100 мм). Разработаны конструкции окон с повышенным звукопоглощением на основе стекло-пакетов с герметизацией воздушного промежутка между стеклами и с заполнением его различными газовыми смесями или создание в нем вакуума. Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения.

Для повышения звукоизоляции в помещениях применяют акустические экраны, устанавливаемые на пути распространения звука на наиболее опасных (с точки зрения разведки) направлениях.

Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. С учетом дифракции эффективность экрана повышается с увеличением соотношения размеров экрана и длины акустической волны. Размеры эффективных экранов превышают более чем в 2-3 раза длину волны. Реально достигаемая эффективность акустического экранирования составляет 8... 10дБ.

Применение акустического экранирования целесообразно при временном использовании помещения для защиты акустической информации. Наиболее часто применяются складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон, технологических проемов, систем кондиционирования, проточной вентиляции и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам.

Для повышения звукоизоляции помещений также применяют звукопоглощающие материалы.

Звукопоглощение обеспечивается путем преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале. Звукопоглощающие свойства материалов оцениваются коэффициентом звукопоглощения, определяемым отношением энергии звуковых волн, поглощенной в материале, к падающей на поверхность материала и проникающей (неотраженной) в звукопоглощающий материал.

Применение звукопоглощающих материалов при защите акустической информации имеет некоторые особенности по сравнению с звукоизоляцией. Одной из особенностей является необходимость создания непосредственно в помещении акустических условий для обеспечения разборчивости речи в различных его зонах. Таким условием является прежде всего обеспечение оптимального соотношения прямого и отраженного от ограждений акустических сигналов. Чрезмерное звукопоглощение приводит к ухудшению уровня сигнала в различных точках помещения, а большое время реверберации - к ухудшению разборчивости в результате наложения различных звуков.

Обеспечение рациональных значений рассмотренных условий определяется как общим количеством звукопоглощающих материалов в помещении, так и распределением звукопоглощающих материалов по ограждающим конструкциям с учетом конфигурации и геометрических размеров помещений.

Звукопоглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными.

Один из распространенных видов пористых материалов - облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит (плиты минераловатные «Акмигран», «Акмант», «Силаклор», «Винипор», ПА/С, ПА/О, ПП-80, ППМ, ПММ) или рельефных конструкций (пирамид, клиньев и т.д.), располагаемых или вплотную, или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.). Используются также звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтового волокна, минеральной ваты) в защитной оболочке из ткани или пленки с перфорированным покрытием (металлическим, гипсовым и др.).

Пористые звукопоглощающие материалы малоэффективны на низких частотах.

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются на мембранные и резонаторные. Мембранные поглотители представляют собой натянутый холст (ткань), тонкий фанерный (картонный) лист, под которым располагают хорошо демпфирующий материал (материал с большой вязкостью, например, поролон, губчатую резину, строительный войлок и т.д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Перфорированные резонаторные поглотители представляют собой систему воздушных резонаторов (например, резонаторов Гельмгольца), в устье которых расположен демпфирующий материал.

Средние значения звукоизоляции некоторых материалов приведены в таблице 5.4.

Повышение звукоизоляции стен и перегородок помещений достигается применением однослойных и многослойных (чаще - двойных) ограждений. В многослойных ограждениях целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон - поролон).

Значения ослабления звука ограждениями, выполненными из некоторых часто применяемых строительных материалов, указаны в таблице 2.6.

Уровень акустического сигнала за ограждением можно приближенно оценить по формуле:

$$R_{or} \approx R_C + 6 + 10 \bullet \lg S_{or} - K_{or}, \text{ дБ}$$

где R_C - уровень речевого сигнала в помещении (перед ограждением), дБ;

$S_{ОГ}$ - площадь ограждения, дБ;

$K_{ОГ}$ - звукоизоляция ограждения, дБ.

Таблица 5.4 - Звукопоглощающие свойства некоторых материалов

Материал	**Коэффициент поглощения на частотах, Гц**					
	125	**250**	**500**	**1000**	**2000**	**4000**
Кирпичная стена	0,024	0,025	0,032	0,041	0,049	0,07
Деревянная обивка	0,1	0,11	0,11	0,08	0,082	0,11
Стекло одинарное	0,03	*	0,027	*	0,02	*
Штукатурка известковая	0,025	0,04	0,06	0,085	0,043	0,058
Войлок (толщина 25 мм)	0,18	0,36	0,71	0,8	0,82	0,85
Ковер с ворсом	0,09	0,08	0,21	0,27	0,27	0,37
Стеклянная вата(толщиной 9 мм)	0,32	0,4	0,51	0,6	0,65	0,6
Хлопчатобумажная ткань	0,03	0,04	0,11	0,17	0,24	0,35

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, коробов, прокладок, глушителей, вязкоупругих заполнителей и т.д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием сложных акустических фильтров и глушителей.

Следует иметь в виду, что в общем случае звукоизоляция ограждающих конструкций, содержащих несколько элементов, должна оцениваться звукоизоляцией наиболее слабого из них.

Таблица 5.5 - Звукопоглощающие свойства некоторых строительных конструкций

Материал	**Толщина**	**Звукоизоляция на частотах (Гц), дБ**					
		125	**250**	**500**	**1000**	**2000**	**4000**
Кирпичная стена	1/2 кирпича	39	40	42	48	54	60
Отштукатуренная с двух сторон стена	1 кирпич	36	41	44	51	58	64
	1,5 кирпича	41	44	48	55	61	65
	2 кирпича	45	45	52	59	65	70
	2,5 кирпича	47	55	60	67	70	70
Стена из железобетонных блоков	40 мм	32	36	35	38	47	53
	100 мм	40	40	44	50	55	60
	200 мм	42	44	51	59	65	65
	300 мм	45	50	58	65	69	69
	400 мм	48	55	61	68	70	70
	800 мм	55	61	68	70	70	70

Стена из шлакоблоков	220 мм	42	42	48	54	60	63
Перегородка из древесно-стружечной плиты	20 см	23	26	26	26	26	26

Для ведения конфиденциальных разговоров разработаны специальные звукоизолирующие кабины. В конструктивном отношении они делятся на каркасные и бескаркасные. В первом случае на металлический каркас крепятся звукопоглощающие панели. Примером таких кабин являются кабины междугородней телефонной связи. Кабины с двухслойными звукопоглощающими плитами обеспечивают ослабление звука до 35... 40 дБ.

Более высокой акустической эффективностью (большим коэффициентом ослабления) обладают кабины бескаркасного типа. Они собираются из готовых многослойных щитов, соединенных между собой через звукоизолирующие упругие прокладки. Такие кабины дороги в изготовлении, но снижение уровня звука в них может достигать 50 ... 55 дБ. Для повышения звукоизоляции кабины минимизируют возможное число стыковочных соединений отдельных панелей между собой и с каркасом кабины. Тщательно герметизируют и уплотняют стыковочные соединения, применяют звукопоглощающие облицовки стен и потолка. В системах вентиляции и кондиционирования воздуха устанавливают специальные глушители звука.

Звукоизолирующие кабины в зависимости от требований к звукоизоляции подразделяются на 4 класса. В диапазоне 63 ... 8000 Гц кабины должны обеспечивать ослабление звука: кабины 1-го класса - на 25 ... 50 дБ; 2-го класса - на 15 ... 49 дБ; 3-го и 4-го классов - 15 ... 39 и 15 ... 29 дБ соответственно. Наименьшие значения соответствуют низким частотам, наибольшие - высоким (2000 ... 4000 Гц).

5.2.2 Виброакустическая маскировка

В случае, если используемые пассивные средства защиты помещений не обеспечивают требуемых норм по звукоизоляции необходимо использовать активные меры защиты.

Активные меры защиты заключаются в создании маскирующих акустических помех средствам разведки, то есть использованием виброакустической маскировки информационных сигналов. В отличие от звукоизоляции помещений, обеспечивающей требуемое ослабление интенсивности звуковой волны за их пределами, использование активной акустической маскировки снижает отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи).

Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброакустическому и оптико-электронному каналам утечки информации.

Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители) или вибрационные излучатели (вибродатчики).

На практике наиболее широкое применение нашли генераторы шумовых колебаний. Именно поэтому активную акустическую маскировку часто называют акустическим зашумлением. Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников

шумов. В качестве источников шумовых колебаний используются электровакуумные, газоразрядные, полупроводниковые и другие электронные приборы и элементы.

Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен и с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемые псевдослучайными.

Наряду с шумовыми помехами в целях активной акустической маскировки используют и другие помехи, например, "одновременный разговор нескольких человек", хаотические последовательности импульсов и т.д.

Роль оконечных устройств, осуществляющих преобразование электрических колебаний в акустические колебания речевого диапазона длин волн, обычно выполняют малогабаритные широкополосные громкоговорители, а осуществляющих преобразование электрических колебаний в вибрационные - вибрационные излучатели (вибродатчики).

Громкоговорители систем зашумления устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки, а вибродатчики крепятся на рамах, стеклах, коробах, трубопроводах, стенах, потолках и т.д.

Создаваемые вибродатчиками шумовые колебания в ограждающих конструкциях, трубах, оконном стекле и т.д. приводят к значительному повышению в них уровня вибрационных шумов и тем самым - к существенному ухудшению условий приема и восстановления речевых сообщений средствами разведки.

В настоящее время создано большое количество различных систем активной виброакустической маскировки, успешно используемых для подавления средств перехвата речевой информации. К ним относятся: системы "Заслон", "Кабинет", "Барон", "Фон-В", VNG-006, ANG-2000, NG-101 и др. (см. табл. 5.6).

В состав типовой системы виброакустической маскировки входят шумогенератор и от 6 до 12 ... 25 вибродатчиков (пьезокерамических или электромагнитных). Дополнительно в состав системы могут включаться звуковые колонки (спикеры).

Таблица 5.6 - Основные характеристики систем виброакустического зашумления

Наименование характеристик	**Модель (тип)**		
	VNG – 006DM	**ANG - 2000**	**«Заслон – 2М»**
Полоса частот эффективной защиты на перекрытии толщиной 0,25 м, кГц	0,25 … 5,0	0,25 … 5,0	0,1 … 5,0
Максимальное количество вибродатчиков, шт.	12	18	25
Тип и принцип действия вибродатчиков	КВП-2, КВП-6, КВП-7пьезокерамические	TRN-2000электромагнитные	электромагнитные
Эффективный радиус подавления вибродатчика на перекрытии толщиной 0,25 м, м	4	5	1,5
Габариты вибродатчиков, мм	Ø 40х30, Ø 50х39, Ø 33х8	Ø 100х338	46х65х53
Примечания	Подключение спикера.	Подключение спикера.	Акустопуск.

	Сертификат Гостехкомиссии России.	Сертификат Гостехкомиссии России.	Адаптация к акустическому фону.

В комплекс "Барон", кроме обычного генератора шума, включены три радиоприемника, независимо настраиваемые на различные радиовещательные станции FM (УКВ-2) диапазона. Смешанные сигналы этих станций используются в качестве помехового сигнала, что значительно повышает эффективность помехи.

Для полной защиты помещения по виброакустическому каналу вибродатчики должны устанавливаться на всех ограждающих конструкциях (стенах, потолке, полу), оконных стеклах, а также трубах, проходящих через помещение. Требуемое количество вибродатчиков для защиты помещения определяется не только его площадью, количеством окон и труб, проходящих через него, но и эффективностью датчиков (эффективный радиус действия вибродатчиков на перекрытии толщиной 0,25 м составляет от 1,5 до 5 м).

В ряде систем виброакустической маскировки возможна регулировка уровня помехового сигнала. Например, в системах "Кабинет" и ANG-2000 осуществляется ручная плавная регулировка уровня помехового сигнала, а в системе "Заслон-2М"- автоматическая (в зависимости от уровня маскируемого речевого сигнала). В комплексе "Барон" возможна независимая регулировка уровня помехового сигнала в трех частотных диапазонах (центральные частоты: 250, 1000 и 4000 Гц).

Для защиты выделенных помещений в основном развертываются стационарные системы виброакустической маскировки, но для защиты временно используемых для проведения закрытых мероприятий могут применяться и мобильные. К таким системам относится, например, мобильная система виброакустического зашумления "Фон-В". В состав системы входят: генератор ANG-2000, вибродатчики TRN-2000 и TRN-2000M и металлические штанги для крепления датчиков к строительным конструкциям.

Система обеспечивает защиту помещения площадью до 25 $м^2$.

Монтаж (демонтаж) системы осуществляется тремя специалистами в течение 30 минут без повреждения строительных конструкций и элементов отделки интерьера.

Для создания акустических помех в небольших помещениях или салоне автомобиля могут использоваться малогабаритные акустические генераторы, например, WNG-023. Генератор имеет размеры 111*70*22 мм и создает помеховый (типа "белый шум") акустический сигнал в диапазоне частот от 100 до 12000 Гц мощностью 1 Вт. Питание генератора осуществляется от элемента типа "Крона" или сети 220 В.

При организации акустической маскировки необходимо помнить, что акустический шум может создавать дополнительный мешающий фактор для сотрудников и раздражающе воздействовать на нервную систему человека, вызывая различные функциональные отклонения и приводить к быстрой и повышенной утомляемости работающих в помещении. Степень влияния мешающих помех определяется санитарными нормативами на величину акустического шума. В соответствии с нормами для учреждений величина мешающего шума не должна превышать суммарный уровень 45 дБ.

5.2.3 Методы и средства обнаружения и подавления диктофонов и акустических закладок

Диктофоны и акустические закладки в своем составе содержат большое количество полупроводниковых приборов, поэтому наиболее эффективным средством их обнаружения является нелинейный локатор, устанавливаемый на входе в выделенное помещение и работающий в составе системы контроля доступа.

К типовым представителям устройств этого класса относится, например, нелинейный локатор "Циклон- Рамка". Локатор имеет два датчика, выносной пульт управления и может скрытно устанавливаться в дверной проем выделенного помещения, что позволяет контролировать наличие у посетителей (как в ручной клади, так и под одеждой) любых радиоэлектронных устройств, в том числе диктофонов и подслушивающих устройств, как во включенном, так и в выключенном состояниях. Зона контроля локатора составляет: по высоте - 2,2 м, по длине - 1,5 м, по ширине -1,5 м.

Для обнаружения работающих в режиме записи диктофонов применяются так называемые ***детекторы диктофонов***. Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи. Электродвижущая сила (ЭДС), наводимая этим полем в датчике сигналов (магнитной антенне), усиливается и выделяется из шума специальным блоком обработки сигналов. При превышении уровня принятого сигнала некоторого установленного порогового значения срабатывает световая или звуковая сигнализация. Во избежание ложных срабатываний порог обнаружения необходимо корректировать практически перед каждым сеансом работы, что является недостатком подобных приборов.

Детекторы диктофонов выпускаются в переносном и стационарном вариантах. К переносным относятся детекторы "Сова", RM-100, TRD-800, а к стационарным - PTRD-14, PTRD-16, PTRD-18 и т.д.

В переносном (носимом) варианте блок анализа детектора размещается в кармане оператора, поисковая антенна в рукаве (обычно крепится на предплечье), а датчик сигнализации вибраторного типа - на поясе или в кармане. В ходе переговоров оператор приближает антенну (руку) к возможным местам установки диктофона (портфель, одежда собеседника и т.д.). При обнаружении излучений (превышении магнитного поля установленного оператором порогового значения) включенного на запись диктофона скрытый сигнализатор-вибратор начинает вибрировать, сигнализируя оператору о возможной записи разговора.

Для защиты выделенных помещений в основном используются детекторы диктофонов, выполненные в стационарных вариантах. В отличие от переносных детекторов, имеющих один датчик сигналов, стационарные детекторы диктофонов оборудованы несколькими датчиками (например, детектор PTRD-18 имеет возможность подключения до 16 датчиков одновременно), что позволяет существенно повысить вероятность обнаружения диктофонов.

Стационарный вариант предполагает установку (заделку) антенн в стол для переговоров и в кресла (подлокотники). Блок анализа и индикатор наличия диктофонов размещается в столе руководителя или у дежурного (в этом случае создается дополнительный канал управления). При наличии у беседующего диктофона в одежде или

в вещах (папка, портфель и т.д.) у руководителя скрытным образом будет срабатывать индикация этого факта.

Ввиду слабого уровня магнитного поля, создаваемого работающими диктофонами (особенно в экранированных корпусах), дальность их обнаружения детекторами незначительна. Например, дальность обнаружения диктофона L- 400 в режиме записи в условиях офиса даже при использовании стационарного детектора PTRD-018 не превышает 45 ... 65 см. Дальность обнаружения диктофонов в неэкранированных корпусах может составлять 1 ... 1,5 м. Основные характеристики детекторов диктофонов представлены в каталоге.

Наряду со средствами обнаружения портативных диктофонов на практике эффективно используются и средства их подавления. Для этих целей используются устройства электромагнитного подавления типа "Рубеж", "Шумотрон", "Буран", "УПД" и др. (таблица 5.7) и устройства ультразвукового подавления типа "Завеса". Основные характеристики устройств подавления диктофонов представлены в каталоге.

Принцип действия устройств электромагнитного подавления основан на генерации в дециметровом диапазоне частот (обычно в районе 900 МГц) мощных шумовых сигналов. В основном для подавления используются импульсные сигналы. Излучаемые направленными антеннами помеховые сигналы, воздействуя на элементы электронной схемы диктофона (в частности, усилитель низкой частоты и усилитель записи), вызывают в них наводки шумовых сигналов. Вследствие этого одновременно с информационным сигналом (речью) осуществляется запись и детектированного шумового сигнала, что приводит к значительному искажению первого.

Зона подавления диктофонов зависит от мощности излучения, его вида, а также от типа используемой антенны. Обычно зона подавления представляет собой сектор с углом от 30 до 80 градусов и радиусом до 1,5 м (для диктофонов в экранированном корпусе).

Устройства подавления диктофонов используют как непрерывные, так и импульсные сигналы. Например, подавитель диктофонов "Шумотрон-2" работает в импульсном режиме на частоте 915 МГц. Длительность излучаемого импульса не более 300 мкс, а импульсная мощность -не менее 150 Вт. При средней мощности излучения 20 Вт обеспечивается дальность подавления диктофонов в экранированном корпусе (типа "Olimpus-400") до 1,5 м в секторе около 30 градусов. Дальность подавления диктофонов в неэкранированном корпусе составляет несколько метров.

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения около 20 кГц), воздействующие непосредственно на микрофоны диктофонов или акустических закладок, что является их преимуществом. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона или акустической закладки (усилитель начинает работать в нелинейном режиме) и тем самым - к значительным искажениям записываемых (передаваемых) сигналов.

В отличие от систем электромагнитного подавления подобные системы обеспечивают подавление в гораздо большем секторе. Например, комплекс "Завеса" при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 $м^3$. Однако системы ультразвукового подавления имеют и один важный недостаток: эффективность их резко снижается, если микрофон диктофона или закладки прикрыть фильтром из специального

материала или в усилителе низкой частоты установить фильтр низких частот с граничной частотой 3,4 ... 4 кГц.

Для обнаружения радиозакладок в выделенных помещениях могут использоваться индикаторы поля, интерсепторы, радиочастотомеры, сканерные приемники, программно-аппаратные комплексы контроля и другие технические средства.

Наиболее эффективным методом выявления радиозакладок в выделенных помещениях является **постоянный** (круглосуточный) **радиоконтроль** с использованием программно-аппаратных комплексов контроля. Для его организации в специально оборудованном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого, как правило, включаются один или несколько программно-аппаратных комплексов, позволяющих контролировать все выделенные помещения. На пункте радиоконтроля устанавливается опорная антенна, а в выделенных (контролируемых) помещениях - малогабаритные широкополосные антенны и звуковые колонки или выносные микрофоны, которые при установке камуфлируются. Антенны и звуковые колонки (или микрофоны) специально проложенными кабелями соединяются соответственно с блоками высокочастотного (антенного) или низкочастотного коммутаторов, установленных в помещении стационарного пункта контроля.

Если при проведении радиоконтроля обнаружена передача информации радиозакладкой, то до ее выявления может быть организована **постановка прицельных помех** на частоте передачи закладки. Для этих целей может использоваться, например, устройство постановки помех АРК-СП.

В состав аппаратуры АРК-СП входят широкополосная антенна, перестраиваемый передатчик помех и программное обеспечение. Управляющая программа позволяет с высокой скоростью настраивать передатчик на предварительно заданные частоты в диапазоне от 65 до 1000 МГц. Передатчик создает прицельную по частоте помеху с узкополосной и широкополосной модуляцией несущей частоты специальными сигналами: речевая фраза или тональный сигнал. Мощность помехи -150 ... 200 мВт. Аппаратура функционирует под управлением ПЭВМ автономно или в составе программно-аппаратных комплексов контроля типа АРК и позволяет осуществлять постановку помех одновременно

Таблица 5.7 - Основные характеристики устройств подавления аппаратуры магнитной записи

Наимено-ваниеие характе-ристик	**Модель (тип)**					
	«Рубеж-1»	**«РаМЗес-Авто»**	**«РаМЗес-Дубль»**	**«Буран-2»**	**«Буран-3»**	**«УПД-2»**
Дальность подавления, м	не менее 1,5/ -	не менее 1,5/ до 1,5	не менее 2/ до 2	не менее 1,5/ -	не менее 3/ 2	до 6 (?)/ до 4 (?)
Зона подавления	Телесный уголне менее 60°	Шаровой сектор с углом не менее 60°	Шаровой сектор с углом не менее 70°	45° • 45°	45° • 45°	Сектор с углом не менее 80°
Излучаемая мощность, Вт	-	5 (АС 220 В)4 (DC 12 В)	8	Не более 10 Вт вимпульсе	Не более 10 Вт в импульсе	-
Питание, потребляемая мощность	АС 220 В, не более 25 Вт	АС 220 В (30 Вт)DC 12 В (20 Вт)	АС 220 В,не более 40 Вт	АС 220 В; DC 12 В, не более 40 Вт	АС 220 В;DC 12 В,не более 40 Вт	АС 220 В; DC 12 В,не более 60 Вт

Время непрерывной работы	не более 1 часа	не более 1 часа	не более 1 часа	не более 2 ч (АС)не более 1 ч (DC)	не более 2 ч (АС)не более 1 ч (DC)	не более 1,5 ч (DC)
Примечания	Стационарный	Стацио-нарный, автомо-бильный	Стационарный. Возможность подключения одной или двух антенн одновременно		В дипломате. Адаптивная модуляция помехового сигнала	В дипломате. Пульт дистанционного управления

Примечание: В графе дальность подавления в числителе – диктофона в пластмассовом корпусе, в знаменателе – в металлическом корпусе.

(попеременно) на четырех частотах (время излучения на одной не менее 50 мс).

Аппаратура питается от сети 220 В и имеет размеры 300*300*55 мм.

Для подавления радиозакладок также могут использоваться системы пространственного электромагнитного зашумления, применяемые для маскировки побочных электромагнитных излучений ТСПИ. Однако при этом необходимо помнить, что ввиду сравнительно низкой спектральной мощности излучаемой помехи, эти системы эффективны только для подавления маломощных (как правило, с мощностью излучения менее 10 мВт) радиозакладок. Поэтому для подавления радиозакладок необходимо использовать генераторы шума с повышенной мощностью.

Для защиты речевой информации от сетевых акустических закладок используются помехоподавляющие фильтры низких частот и системы линейного зашумления.

Помехоподавляющие фильтры устанавливаются в линии питания розеточной и осветительной сетей в местах их выхода из выделенных помещений. Учитывая, что сетевые закладки используют для передачи информации частоты свыше 40 ... 50 кГц, для защиты информации необходимо использовать фильтры низких частот с граничной частотой не более 40 кГц. К таким фильтрам относятся, например, фильтры типа ФСПК, граничная частота которых составляет 20 кГц.

В системах зашумления линий электропитания используются генераторы шума типа "Гром-ЗИ-4", "Гром-ЗИ-6Ц", "Гном-2С" и др. Основные характеристики генераторов шума представлены в каталоге.

При выборе генераторов шума особое внимание необходимо уделять полосе частот и спектральной мощности помехового сигнала. Например, генераторы шума "Гром-ЗИ-4", "Гром-ЗИ-6Ц" создают помеховый сигнал в диапазоне частот от 0,1 до 1 МГц и от 0,1 до 5 МГц соответственно. Поэтому они не эффективны для подавления сетевых закладок, использующих для передачи информации частоты ниже 100 кГц

5.2.4 Методы и средства защиты телефонных линий

При защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:

- телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;
- телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;
- и, конечно, возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, имеющих способность преобразовывать акустические колебания в электрические, то есть обладающих "микрофонным эффектом". К ним относятся: звонковая цепь, телефонный и, конечно, микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы.

При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода "высокочастотного навязывания", несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом.

Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для защиты телефонного аппарата от утечки акустической (речевой) информации по электроакустическому каналу используются как пассивные, так и активные методы и средства.

К наиболее широко применяемым пассивным методам защиты относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- отключение преобразователей (источников) опасных сигналов.

Возможность **ограничения опасных сигналов** основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречно-включенных диода. Такие диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и единицы Ом и менее - для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов.

Диодные ограничители включаются последовательно в линию звонка (см. рис. 5.1) или непосредственно в каждую из телефонных линий (см. рис. 5.3).

Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания".

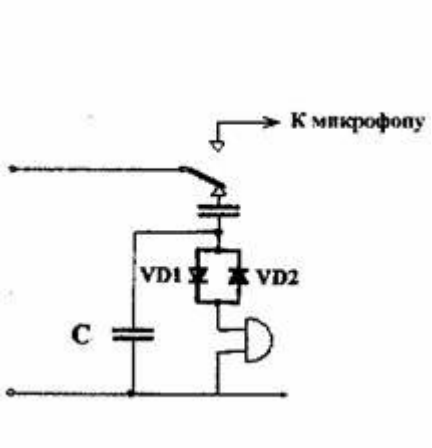


Рисунок 5.1 - Схема защиты звонковой цепи

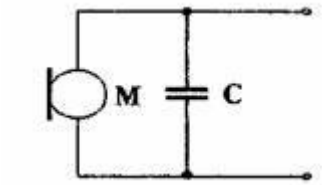


Рисунок 5.2- Схема защиты микрофона телефонного аппарата

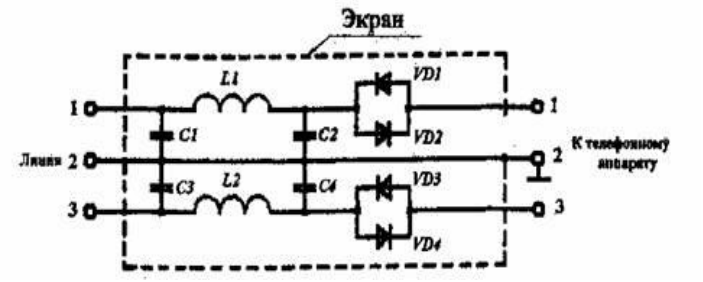


Рисунок 5.3 - Схема устройства защиты телефонных аппаратов типа «Гранит», сочетающего фильтр и ограничитель

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов (см. рис. 5.1, 5.2). Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказывать существенного влияния на полезные сигналы. Обычно для установки в звонковую цепь используются конденсаторы емкостью 1 мкФ, а для установки в микрофонную цепь - емкостью 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах.

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель. К ним относятся: устройства типа "Экран", "Гранит-8", "Корунд", "Грань-300" и др. (см. рис. 5.3).

Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты информации.

Самый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, включаемого и выключаемого вручную. Более удобным в эксплуатации является установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке.

К типовым устройствам, реализующим данный метод защиты, относится изделие "Барьер- Ml". В его состав входят:

- электронный коммутатор;
- схема анализа состояния телефонного аппарата, наличия вызывных сигналов и управления коммутатором;
- схема защиты телефонного аппарата от воздействия высоковольтных импульсов.

Устройство работает в следующих режимах: дежурном, передачи сигналов вызова и рабочем.

В дежурном режиме (при положенной телефонной трубке) телефонный аппарат отключен от линии, и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При этом сопротивление развязки между телефонным аппаратом и линией АТС составляет не менее 20 МОм. Напряжение на выходе устройства в дежурном приеме составляет 5...7В.

При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии. Подключение осуществляется только на время действия сигналов вызова.

При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии. Переход устройства из дежурного в рабочий режим осуществляется при токе в телефонной линии не менее 5 мА.

Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного (защищаемого) помещения или в распределительном щитке (кроссе), находящемся в пределах контролируемой зоны.

Электропитание устройства осуществляется от телефонной линии при токе потребления в дежурном режиме не более 0,3 мА.

Устройство "Барьер –М1" обеспечивает защиту телефонного аппарата не только от утечки информации по электроакустическому каналу, но также и его защиту от воздействия высоковольтных импульсов (напряжением до 1000 В и длительностью до 100 мкс).

Активные методы защиты от утечки информации по электроакустическому каналу предусматривают линейное зашумление телефонных линий. Шумовой сигнал подается в

линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается.

К сертифицированным средствам линейного зашумления относятся устройства МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц П-1А (защита цифровых телефонных аппаратов) и др.

Для защиты акустической (речевой) информации в выделенных помещениях наряду с защитой телефонных аппаратов необходимо принимать меры и для защиты непосредственно телефонных линий, так как они могут использоваться в качестве источников питания акустических закладок, установленных в помещениях, а также для передачи информации, получаемой этими закладками.

При этом используются как пассивные, так и активные методы и средства защиты. Пассивные методы защиты основаны на блокировании акустических закладок, питающихся от телефонной линии в режиме положенной трубки, а активные - на линейном зашумлении линий и уничтожении (электрическом "выжигании") закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов.

Защита телефонных разговоров от перехвата осуществляется главным образом активными методами. К основным из них относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления");
- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод "выжигания").

Суть **метода синфазной маскирующей низкочастотной (НЧ) помехи** заключается в подаче в каждый провод телефонной линии с использованием единой системы заземления аппаратуры АТС и нулевого провода электросети 220 В (нулевой провод электросети заземлен) согласованных по амплитуде и фазе маскирующих сигналов речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (телефонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значительно превосходит полезный сигнал, то перехват информации (выделение полезного сигнала) становится невозможным.

В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности импульсов).

Метод синфазного маскирующего низкочастотного сигнала используется для подавления телефонных радиозакладок (как с параметрической, так и с кварцевой стабилизацией частоты) с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) с помощью индукционных датчиков различного типа.

Метод **высокочастотной маскирующей помехи** заключается в подаче во время разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового диапазона.

Данный метод используется для подавления практически всех типов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индукционных датчиков. Однако эффективность подавления средств съема информации с подключением к линии при помощи с индукционных датчиков (особенно не имеющих предусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа "белого шума" или дискретные сигналы типа псевдослучайной последовательности импульсов.

Частоты маскирующих сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора закладки или микрофонного усилителя диктофона их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал. Обычно используются частоты в диапазоне от 6 ... 8 кГц до 16 ... 20 кГц. Например, в устройстве Sel SP-17/T помеха создается в диапазоне 8 ... 10 кГц.

Такие маскирующие помехи вызывают значительные уменьшение отношения сигнал/шум и искажения полезных сигналов (ухудшение разборчивости речи) при перехвате их всеми типами подслушивающих устройств. Кроме того, у радиозакладок с параметрической стабилизацией частоты ("мягким" каналом) как последовательного, так и параллельного включения наблюдается "уход" несущей частоты, что может привести к потере канала приема.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов. Аналогичную роль выполняют полосовые фильтры, установленные на городских АТС, пропускающие сигналы, частоты которых соответствуют стандартному телефонному каналу (300 Гц ... 3,4 кГц), и подавляющие помеховый сигнал.

Метод ультразвуковой маскирующей помехи в основном аналогичен рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20 ...25 кГц до 50... 100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиозакладок. Поднятие напряжения в линии до 18 ... 24 В вызывает у радиозакладок с последовательным подключением и параметрической стабилизацией частоты "уход" несущей частоты и ухудшение разборчивости речи вследствие размытия спектра сигнала. У радиозакладок с последовательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3 ... 10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод "обнуления" предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод используется для нарушения функционирования подслушивающих устройств с контактным параллельным подключением к линии и использующих ее в качестве источника питания. К таким устройствам относятся: параллельные телефонные аппараты, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, акустические и телефонные закладки с питанием от телефонной линии и т.д.

Метод низкочастотной маскирующей помехи заключается в подаче в линию при положенной телефонной трубке маскирующего сигнала (наиболее часто, типа "белого шума") речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц) и применяется для подавления проводных микрофонных систем, использующих телефонную линию для передачи информации на низкой частоте, а также для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (то есть при отсутствии полезного сигнала).

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии.

Суть метода заключается в следующем. При передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого диапазона с известным спектром). Одновременно этот же маскирующий сигнал ("чистый" шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи.

Недостатком данного метода является то, что маскировка речевых сообщений односторонняя и не позволяет вести двухсторонние телефонные разговоры.

Метод "выжигания" реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

При использовании данного метода телефонный аппарат от линии отключается. Подача импульсов в линию осуществляется два раза. Первый (для "выжигания" параллельно подключенных устройств) - при разомкнутой телефонной линии, второй (для "выжигания" последовательно подключенных устройств) - при закороченной (как правило, в центральном распределительном щитке здания) телефонной линии.

Для защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную защиту линий различными методами, включая защиту от утечки информации по электроакустическому каналу.

На отечественном рынке имеется большое разнообразие средств защиты. Среди них можно выделить следующие: "SP 17/T", "SI-2001", "КТЛ-3","КТЛ-400", "Ком-3", "Кзот-06", "Цикада-М", "Прокруст" (ПТЗ-003), "Прокруст-2000", "Консул", "Гром-ЗИ-6", "Протон" и др. Основные характеристики некоторых из них приведены в таблице 4.9.

В активных устройствах защиты телефонных линий наиболее часто реализованы метод высокочастотной маскирующей помехи ("SP 17/T", "КТЛ-3","КТЛ-400", "Ком-3", "Прокруст" (ПТЗ-003), "Прокруст-2000","Гром-ЗИ-6", "Протон" и др.) и метод ультразвуковой маскирующей помехи ("Прокруст" (ПТЗ-003), "Гром-ЗИ-6").

Метод синфазной низкочастотной маскирующей помехи используется в устройстве "Цикада-М", а метод низкочастотной маскирующей помехи - в устройствах "Прокруст", "Протон", "Кзот-06" и др.

Метод "обнуления" применяется, например, в устройстве "Цикада-М", а метод повышения напряжения в линии - в устройстве "Прокруст".

Компенсационный метод маскировки речевых сообщений, передаваемых абоненту по телефонной линии, реализован в изделии "Туман".

Большинство устройств защиты производят автоматическое измерение напряжения в линии и отображают его значение на цифровом индикаторе. В приборе "Гром-ЗИ-6" на цифровом индикаторе отображается уровень уменьшения напряжения в линии.

Устройства защиты телефонных линий имеют сравнительно небольшие размеры и вес (например, изделие "Прокруст" при размерах 62*155*195 мм весит 1 кг). Питание их, как правило, осуществляется от сети переменного тока 220 В. Однако некоторые устройства (например, "Кзот-06") питаются от автономных источников питания.

Для вывода из строя ("выжигания" входных каскадов) средств несанкционированного съема информации с гальваническим подключением к телефонной линии используются устройства типа "ПТЛ-1500, "КС-1300", КС-1303", "Кобра" и т.д.

Приборы используют высоковольтные импульсы напряжением не менее 1500 ... 1600 В. Мощность "выжигающих" импульсов составляет 15 ... 50 ВА. Так как в схемах закладок применяются миниатюрные низковольтные детали, то высоковольтные импульсы их пробивают и схема закладки выводится из строя.

"Выжигатели" телефонных закладок могут работать как в ручном, так и автоматическом режимах. Время непрерывной работы в автоматическом режиме составляет от 20 секунд до 24 часов.

Таблица 5.8 - Основные характеристики устройств активной защиты телефонной линии

Наименование характеристик	Тип устройства					
	«Прокруст»	«Протон»	«Цикада-М»	Sel SP-17/P	Гром-ЗИ-6	Кзот-06
Метод синфазной низкочастотной маскирующей помехи	-	-	•	-	-	-
Метод высокочастотной маскирующей помехи	•	•	-	•	•	•
Метод ультразвуковой маскирующей помехи	-	-	•	-	•	-
Метод повышения напряжения	•	-	-	-	-	-
Метод "обнуления"			•	-	-	-
Метод низкочастотной маскирующей помехи	•	•	-	-	-	•
Метод "выжигания"	-	-	-	-	-	-
Индикация	световая	световая	световая	световая	световая, звуковая	световая
Габаритные размеры, мм	62*155*195	205*60*285	68*176*170	152*104*34	150*200*50	210*85*32
Вес, кг	1	2,3		0,6	1,5	0.75
Напряжение питания, В	220	220	220	220/12	220	9
Примечание	Цифровая индикация напряжения в линии	Цифровая индикация напряжения в линии		Частотный диапазон помехи8 … 10 кГ. Уровень сигнала помехи 70 дБ	Цифровая индикация уменьшения напряжения в линии	Цифровая индикация напряжения в линии

Устройство «КС-1300» оборудовано специальным таймером, позволяющим при работе в автоматическом режиме устанавливать временной интервал подачи импульсов в линию в пределах от 10 минут до 2 суток.

Наряду со средствами активной защиты на практике широко используются различные устройства, позволяющие контролировать некоторые параметры телефонных линий и устанавливать факт несанкционированного подключения к ним.

Методы контроля телефонных линий в основном основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии.

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряжение, соответствующее нормальному состоянию линии (когда к линии не подключены посторонние устройства), и порог тревоги. При уменьшении напряжения в линии более установленного порога устройством подается световой или звуковой сигнал тревоги.

На принципах измерения напряжения в линии построены и устройства, сигнализирующие о размыкании телефонной линии, которое возникает при последовательном подключении закладного устройства.

Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет "микрофонного эффекта" в элементах телефонного аппарата и высокочастотного "навязывания".

Устройства контроля телефонных линий, построенные на рассмотренном принципе, реагируют на изменения напряжения, вызванные не только подключением к линии средств съема информации, но и колебаниями напряжения на АТС (что для отечественных линий довольно частое явление), что приводит к частым ложным срабатываниям сигнализирующих устройств. Кроме того, эти устройства не позволяют выявить параллельное подключение к линии высокоомных (с сопротивлением в несколько МОм) подслушивающих устройств. Поэтому подобные устройства не находят широкого применения на практике.

Принцип работы более сложных устройств основан на периодическом измерении и анализе нескольких параметров линии (наиболее часто: напряжения, тока, а также комплексного (активного и реактивного) сопротивления линии). Такие устройства позволяют определить не только факт подключения к линии средств съема информации, но и способ подключения (последовательное или параллельное). Например, контроллеры телефонных линий "КТЛ-2", "КТЛ-3" и "КТЛ-400" за 4 минуты позволяют обнаружить закладки с питанием от телефонной линии независимо от способа, места и времени их подключения, а также параметров линии и напряжения АТС. Приборы также выдают световой сигнал тревоги при кратковременном (не менее 2 секунд) размыкании линии.

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съема информации, оборудованы и средствами их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

Для **блокировки работы (набора номера)** несанкционированно подключенных **параллельных телефонных аппаратов** используются **специальные электронные блокираторы**.

Принцип работы подобных устройств состоит в следующем. В дежурном режиме устройство защиты производит анализ состояния телефонной линии путем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппарате снята), срабатывает звуковая и световая (загорается светодиод несанкционированного подключения к линии) сигнализация. А если факт несанкционированного подключения к линии зафиксирован в отсутствии телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнализация и устройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата. В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя

снятие трубки на защищаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата.

Кроме несанкционированного подключения к линии параллельного телефонного аппарата подобные устройства сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.

5.3 Методы и средства защиты информации от перехвата компьютерной информации

Защита информации, обрабатываемой техническими средствами, осуществляется с применением **пассивных** и **активных** методов и средств.

Пассивные методы защиты информации направлены на:

- ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Активные методы защиты информации направлены на:

- создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;
- создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного cm-нала ТСПИ.

Ослабление побочных электромагнитных излучений ТСПИ и их наводок в посторонних проводниках осуществляется путем экранирования и заземления ТСПИ и их соединительных линий.

Исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания достигается путем фильтрации информационных сигналов.

Для создания маскирующих электромагнитных помех используются системы пространственного и линейного зашумления.

5.3.1 Экранирование

Функционирование любого технического средства информации связано с протеканием по его токоведущим элементам электрических токов различных частот и

образованием разности потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля, называемые **побочными электромагнитными излучениями.**

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей или последняя много меньше магнитной за счет свойств излучателя.

Переменные электрическое и магнитное поля создаются также в пространстве, окружающем соединительные линии (провода, кабели) ТСПИ.

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования:

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и магнитостатическое экранирование основаны на замыкании экраном (обладающим в первом случае высокой электропроводностью, а во втором - магнитопроводностью) соответственно электрического и магнитного полей.

Электростатическое экранирование по существу сводится к замыканию электростатического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля. При использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника наводки в Е раз, где Е - относительная диэлектрическая проницаемость материала экрана.

Основной задачей экранирования электрических полей является снижение емкости связи между экранируемыми элементами конструкции. Следовательно, эффективность экранирования определяется в основном отношением емкостей связи между источником и

рецептором наводки до и после установки заземленного экрана. Поэтому любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования.

Экранирующее действие металлического листа существенно зависит от качества соединения экрана с корпусом прибора и частей экрана друг с другом. Особенно важно не иметь соединительных проводов между частями экрана и корпусом.

В диапазонах метровых и более коротких длин волн соединительные проводники длиной в несколько сантиметров могут резко ухудшить эффективность экранирования. На еще более коротких волнах дециметрового и сантиметрового диапазонов соединительные проводники и шины между экранами недопустимы. Для получения высокой эффективности экранирования электрического поля здесь необходимо применять непосредственное сплошное соединение отдельных частей экрана друг с другом.

Узкие щели и отверстия в металлическом экране, размеры которых малы по сравнению с длиной волны, практически не ухудшают экранирование электрического поля.

С увеличением частоты эффективность экранирования снижается.

Основные требования, которые предъявляются к электрическим экранам, можно сформулировать следующим образом:

- конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;
- в области низких частот (при глубине проникновения (б) больше толщины (d), т.е. при б > d) эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;
- в области высоких частот (при d < б) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование используется при необходимости подавить наводки на низких частотах от 0 до 3...10 кГц.

Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

- магнитная проницаемость μа материала экрана должна быть возможно более высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);
- увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;
- стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;
- заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Экранирование высокочастотного магнитного поля основано на использовании магнитной индукции, создающей в экране переменные индукционные вихревые токи (токи Фуко). Магнитное поле этих токов внутри экрана будет направлено навстречу возбуждающему полю, а за его пределами - в ту же сторону, что и возбуждающее поле. Результирующее поле оказывается ослабленным внутри экрана и усиленным вне его. Вихревые токи в экране распределяются неравномерно по его сечению (толщине). Это вызывается явлением поверхностного эффекта, сущность которого заключается в том, что переменное магнитное поле ослабевает по мере проникновения в глубь металла, так как внутренние слои экранируются вихревыми токами, циркулирующими в поверхностных слоях.

Благодаря поверхностному эффекту плотность вихревых токов и напряженность переменного магнитного поля по мере углубления в металл падает по экспоненциальному закону.

Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Чем ниже частота, тем слабее действует экран, тем большей толщины приходится его делать для достижения одного и того же экранирующего эффекта. Для высоких частот, начиная с диапазона средних волн, экран из любого металла толщиной 0,5 ... 1,5 мм действует весьма эффективно. При выборе толщины и материала экрана следует учитывать механическую прочность, жесткость, стойкость против коррозии, удобство стыковки отдельных деталей и осуществления между ними переходных контактов с малым сопротивлением, удобство пайки, сварки и пр.

Для частот выше 10 МГц медная и тем более серебряная пленка толщиной более 0,1 мм дает значительный экранирующий эффект. Поэтому на частотах выше 10 МГц вполне допустимо применение экранов из фольгированного гетинакса или другого изоляционного материала с нанесенным на него медным или серебряным покрытием.

При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

На высоких частотах применяется исключительно **электромагнитное экранирование**. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления. Теория и практика показывают, что с точки зрения стоимости материала и простоты изготовления преимущества на стороне экранированного помещения из листовой стали. Однако при применении сетчатого экрана могут значительно упроститься вопросы вентиляции и освещения помещения. В связи с этим сетчатые экраны также находят широкое применение.

Для изготовления экрана целесообразно использовать следующие материалы:

- сталь листовая декапированная ГОСТ 1386-47 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;

- сетка стальная тканая ГОСТ 3826-47 номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
  сетка стальная плетеная ГОСТ 5336-50 номер 3; 4; 5; 6;
- сетка из латунной проволоки марки Л-80 ГОСТ 6613-53 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Металлические листы или полотнища сетки должны быть между собой электрически соединены по всему периметру. Для сплошных экранов это может быть осуществлено электросваркой или пайкой. Шов электросварки или пайки должен быть непрерывным с тем, чтобы получить цельносварную конструкцию экрана,

Для сетчатых экранов пригодна любая конструкция шва, обеспечивающая хороший электрический контакт между соседними полотнищами сетки не реже чем через 10 ... 15 мм. Для этой цели может применяться пайка или точечная сварка.

Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой 2,5 ... 3 мм, дает ослабление порядка 55 ... 60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) - около 90 дБ. Экран, изготовленный из одинарной медной сетки с ячейкой 2,5 мм, имеет ослабление порядка 65 ... 70 дБ. Необходимая эффективность экрана в зависимости от его назначения и величины уровня излучения ПЭМИН обычно находится в пределах 60... 120 дБ.

Наряду блоками аппаратуры экранированию подлежат и монтажные провода и соединительные линии.

Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки должно осуществляться путем непосредственного контакта (лучше всего путем пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания обратного тока.

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

На низких частотах приходится использовать более сложные схемы экранирования - коаксиальные кабели с двойной оплеткой (триаксильные кабели).

На более высоких частотах, когда толщина экрана значительно превышает глубину проникновения поля, необходимость в двойном экранировании отпадает. В этом случае внешняя поверхность играет роль электрического экрана, а по внутренней поверхности протекают обратные токи.

Применение экранирующей оболочки существенно увеличивает емкость между проводом и корпусом, что в большинстве случаев нежелательно. Экранированные

провода более громоздки и неудобны при монтаже, требуют предохранения от случайных соединений с посторонними элементами и конструкциями.

Длина экранированного монтажного провода должна быть меньше четверти длины самой короткой волны передаваемого по проводу спектра сигнала. При использовании более длинных участков экранированных проводов необходимо иметь в виду, что в этом случае экранированный провод следует рассматривать как длинную линию, которая во избежании искажений формы передаваемого сигнала должна быть нагружена на сопротивление, равное волновому.

Для уменьшения взаимного влияния монтажных цепей следует выбирать длину монтажных высокочастотных проводов наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а неэкранированные провода высокочастотных цепей - при пересечении под прямым углом. При параллельном расположении такие провода должны быть максимально удалены друг от друга или разделены экранами, в качестве которых могут быть использованы несущие конструкции электронной аппаратуры (кожух, панель и т.д.). Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Экраны при этом могут быть однослойными и многослойными комбинированными, изготовленными из свинца, меди, стали, алюминия и их сочетаний (алюминий-свинец, алюминий-сталь, медь-сталь-медь и т.д.).

В кабелях с наружными пластмассовыми оболочками применяют экраны ленточного типа в основном из алюминиевых, медных и стальных лент, накладываемых спирально или продольно вдоль кабеля.

В области низких частот корпуса применяемых многоштырьковых низкочастотных разъемов являются экранами и должны иметь надежный электрический контакт с общей шиной или землей прибора, а зазоры между разъемом и корпусом должны быть закрыты электромагнитными уплотняющими прокладками.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению с используемыми высокочастотными разъемами. При заделке коаксиального кабеля в высокочастотные разъемы жила кабеля не должна иметь натяжения в месте соединения с контактом разъема, а сам кабель должен быть жестко прикреплен к шасси аппаратуры вблизи разъема.

Для эффективного экранирования низкочастотных полей применяются экраны, изготовленные из ферромагнитных материалов с большой относительной магнитной проницаемостью. При наличии такого экрана линии магнитной индукции проходят в основном по его стенкам, которые обладают малым сопротивлением по сравнению с воздушным пространством внутри экрана.

Качество экранирования таких полей зависит от магнитной проницаемости экрана и сопротивления магнитопровода, которое будет тем меньше, чем толще экран и меньше в нем стыков и швов, идущих поперек направления линий магнитной индукции.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи.

Для защиты линий связи от наводок необходимо разместить линию в экранирующую оплетку или фольгу, заземленную в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления.

Для защиты линии связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводами линии. Если линия представляет собой одиночный провод, а возвратный ток течет по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, то их необходимо скрутить, образовав бифиляр (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, в которых по оплетке протекает возвратный ток, также отвечают требованию минимизации площади контура линии.

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксильного кабеля (изолированного коаксильального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского много-проводного кабеля, покрытого с одной или обеих сторон медной фольгой).

Приведем несколько схем, используемых на частотах порядка 100 кГц. Цепь, показанная на рис. 5.4а, имеет большую площадь петли, образованной "прямым" проводом и "землей". Эта цепь подвержена прежде всего магнитному влиянию. Экран заземлен на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем равным 0 дБ для сравнения с затуханием схем на рис. 5.4.б-и.

Схема на рис. 5.4б практически не уменьшает магнитную связь, так как обратный провод заземлен с обоих концов, и в этом смысле она аналогична схеме на рис 5.4.а. Степень улучшения соизмерима с погрешностью расчета (измерения).

Схема на рис. 5.4 в отличается от схемы на рис. 5.4 а наличием обратного провода-коаксиального экрана, однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с "землей" образуется петля большой площади.

Схема на рис. 5.4 г позволяет существенно повысить защищенность цепи (- 49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой на рис. 5.4.б) петли нет, поскольку правый конец цепи не заземлен.

Дальнейшее повышение защищенности цепи достигается применением схемы на рис. 5.4.с, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара на рис. 5.4.г.

Площадь петли в схеме на рис. 5.4.д не больше, чем в схеме на рис. 5.4 .г, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом.

Схема на рис. 5.4.е позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Кроме того, в этой схеме используется независимый экран.

Схема на рис. 5.4ж имеет ту же защищенность, что и схема на рис. 5.4.е: эффект тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны.

Причины улучшения защищенности схемы на рис. 5.4.з по сравнению с рис. 5.4.ж объяснить трудно. Возможной причиной может быть уменьшение площади эквивалентной петли.

Более плотная скрутка проводов (схема рис. 5.4и) позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь (в обоих проводах токи наводятся одинаково).

Для уменьшения магнитной и электрической связи между проводами необходимо уменьшить площадь петли, максимально разнести цепи и максимально уменьшить длину параллельного пробега линий ТСПИ и посторонними проводниками.

При нулевых уровнях сигналов (0 dB) в соединительных линиях ТСПИ между ними и посторонними проводниками должно обеспечиваться переходное затухание не менее 114 dB (13 Нп). Данное переходное затухание обеспечивается, как правило, при прокладке кабелей ТСПИ на расстоянии не менее 0,1 м от посторонних проводников. При этом допускается прокладка кабелей ТСПИ вплотную с посторонними проводниками при суммарной длине их совместного пробега не более 70 м.

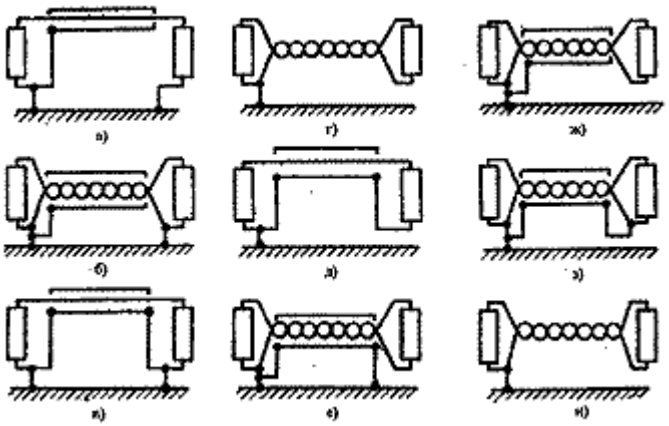


Рисунок 5.4 - Сравнение защищенности различных цепей от влияния внешних магнитных и электрических цепей:

а) 0 дБ; б) -2 дБ; в) -5 дБ; г) - 49 дБ, скрученная пара, 18 витков на метр; д) - 57 дб; е) - 64 дБ, схема предпочтительна на высоких частотах; ж) - 64 дБ; з) - 71 дБ; и) - 79 дБ, скрученная пара (54 витка на метр)

Экранироваться могут не только отдельные блоки (узлы) аппаратуры и их соединительные линии, но и помещения в целом.

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующие свойства дверей и окон хуже.

Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе:

- токопроводящие лакокрасочные покрытия или токопроводящие обои;
- шторы из металлизированной ткани;
- металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

В помещении экранируются стены, двери и окна.

При закрытии двери должен обеспечиваться надежный электрический контакт со стенками помещения (с дверной рамой) по всему периметру не реже чем через 10 ... 15 мм. Для этого может быть применена пружинная гребенка из фосфористой бронзы, которую укрепляют по всему внутреннему периметру дверной рамы.

Окна должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2*2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя сетки должны иметь хороший электрический контакт со стенками помещения (с рамой) по всему периметру. Сетки удобнее делать съемными и металлическое обрамление съемной части также должно иметь пружинящие контакты в виде гребенки из фосфористой бронзы.

При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нормальные условия для работающего в нем человека, прежде всего вентиляцию воздуха и освещение.

Конструкция экрана для вентиляционных отверстий зависит от диапазона частот. Для частот менее 1000 МГц применяются сотовые конструкции, закрывающие вентиляционное отверстие, с прямоугольными, круглыми, шестигранными ячейками. Для достижения эффективного экранирования размеры ячеек должны быть менее одной десятой от длины волны. При повышении частоты необходимые размеры ячеек могут быть столь малыми, что ухудшается вентиляция.

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах, в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Размеры экранированного помещения выбирают исходя из его назначения и стоимости. Обычно экранированные помещения строят площадью 6...8 м2 при высоте 2,5...3 м.

5.3.2 Заземление технических средств

Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

На рис. 5.5 представлена одноточечная последовательная схема заземления.

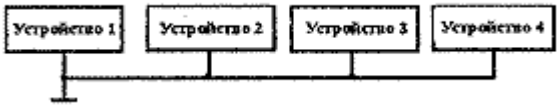


Рисунок 5.5 - Одноточечная последовательная схема заземления

Эта схема наиболее проста. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления (рис. 5.6) этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

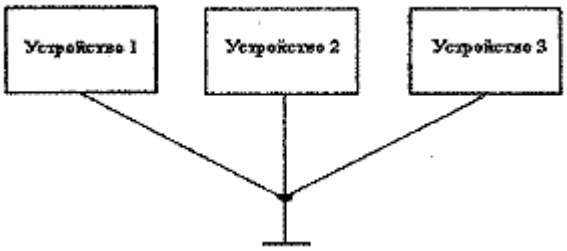


Рисунок 5.6 - Одноточечная параллельная схема заземления

Многоточечная схема заземления (рис.5.7) практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

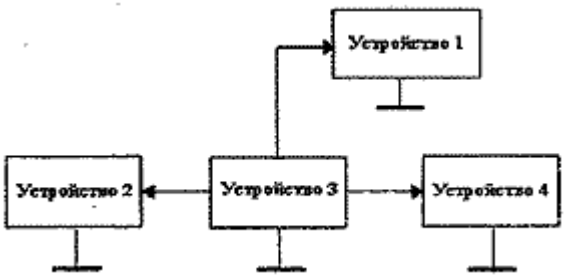


Рисунок 5.7 - Многоточечная схема заземления

Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5•λ. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинированная (гибридная) система заземления, представляющая собой различные сочетания одноточечной, многоточечной и плавающей заземляющих систем.

Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивления заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
- качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;
- контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации и т.д.

Сопротивление заземления определяется главным образом сопротивлением растекания тока в земле. Величину этого сопротивления можно значительно понизить за счет уменьшения переходного сопротивления между заземлителем и почвой путем тщательной очистки перед укладкой поверхности заземлителя и утрамбовкой вокруг него почвы, а также подсыпкой поваренной соли.

Таким образом, величина сопротивления заземления будет в основном определяться сопротивлением грунта.

Удельное сопротивление различных грунтов (т.е. электрическое сопротивление 1 $см^3$ грунта) зависит от влажности почвы, ее состава, плотности, температуры и т.п.. и колеблется в очень широких пределах (см. табл. 5.9).

Таблица 5.9 - Значения удельного сопротивления различных грунтов

Тип грунта	Удельное сопротивление (р), Ом/си3		
	реднее	**мини мальное**	**макси мальное**
Золы, шлаки, соляные отходы	370	500	7000

Глина, суглинки, сланцы	060	340	16300
То же с примесями песка	5800	1020	135 000
Гравий, песок, камни с небольшим количеством глины или суглинков	4000	59000	458 000

Хорошо проводящие грунты теряют свои свойства при отсутствии влаги. Для большинства грунтов 30 % содержания влаги достаточно для обеспечения малого сопротивления. Например, для суглинков удельное сопротивление при влажности 5 % составляет 165000 Ом/см^3, а при влажности 30 % - 6400 Ом/см^3.

При промерзании сопротивление грунтов резко возрастает. Например, для суглинков удельное сопротивление при влажности 15 % и температуре 20 °С составляет 7200 Ом/см^3, при температуре -5 °С - 79000 Ом/см^3, а при температуре -15 °С - 330000 Ом/см^3.

Орошение почвы вокруг заземлителей 2...5 процентным соляным раствором значительно (в 5...10 раз) снижает сопротивление заземления.

Учесть все факторы, влияющие на проводимость почвы, аналитическим путем практически невозможно, поэтому при устройстве заземления величину удельного сопротивления грунта в тех местах, где предполагается размещение заземления, определяют опытным путем.

Как правило, измерение сопротивления заземления проводится два раза в год (зимой и летом).

Если заземлитель состоит из металлической пластины радиуса r, расположенной непосредственно у поверхности земли, то сопротивление заземления $R_З$ можно рассчитать по формуле

$$R_З = \rho / (4 \bullet r_П) \text{, Ом,}$$

где ρ - удельное сопротивление грунта, Ом/см^3;

$r_п$ - радиус пластины, см.

При увеличении глубины закапывания $l_З$ пластины сопротивление заземления уменьшается и при $l_З$ значительно больше r ($l_З$ » r) величина $R_З$ уменьшается в два раза.

Довольно часто применяют заземляющее устройство в виде вертикально вбитой трубы. Сопротивление заземления в этом случае определяется формулой

$$R_З = \left[\rho / (2 \bullet \pi \bullet l)\right] \bullet \left[\ln (4 \bullet l / r_Т) - 1\right] \text{, Ом,}$$

где l - длина трубы, см;

$r_Т$ - радиус трубы, см.

Из формулы видно, что сопротивление заземления зависит в большей степени не от радиуса трубы, а от ее длины. Поэтому при устройстве заземления целесообразнее применять тонкие и длинные трубы (стержни из арматуры).

В табл. 5.10 приведены экспериментально полученные значения сопротивления заземления стержневого заземлителя (0 15,9 мм, 1 = 1,5 м) для различных грунтов.

В качестве одиночных стержневых заземлителей целесообразно использовать медные заземляющие стержни.

Как видно из табл. 5.10, сопротивление простых одиночных заземлителей оказывается достаточно большим. Поэтому такие заземлители находят применение при невысоких требованиях к заземляющим устройствам или при почвах с очень большой проводимостью.

Таблица 5.10 - Значения сопротивления заземления стержневого заземлителя (Ø 15,9 мм, l = 1,5 м) для различных грунтов

Тип грунта	**Сопротивление заземления R_3, Ом**		
	реднее	**мини мальное**	**макси мальное**
Золы, шлаки, соляные отходы	4	3,5	41
Глина, суглинки, сланцы	4	2	98
То же с примесями песка	3	6	800
Гравий, песок, камни с небольшим количеством глины или суглинков	54	35	2700

При повышенных требованиях к величине сопротивления заземления (сопротивление заземления ТСПИ не должно превышать 4 Ом) применяют многократное заземление, состоящее из ряда одиночных симметрично расположенных заземлителей, соединенных между собой.

На практике наиболее часто в качестве заземлителей применяют:

- стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
- сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

При необходимости устройства высокочастотного заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления Z_S складывается из высокочастотного сопротивления магистрали заземления Z_M (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого заземлителя Z_3 (провода, металлического стержня или листа, находящегося в земле).

Величина заземления в основном определяется не сопротивлением заземления, а сопротивлением заземляющей магистрали. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющей магистрали, что достигается за счет уменьшения ее длины и изготовления магистрали в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей магистрали можно сделать весьма небольшой или использовать ее для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно значительно уменьшить величину сопротивления заземлителя $Z_З$. Уменьшить величину $Z_З$ можно также многократным заземлением из симметрично расположенных заземлителей.

При этом общее сопротивление заземления будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2 ... 3 м и диаметром 35 ... 50 мм и стальные полосы сечением 50 ... 100 мм.

Наиболее пригодными являются трубы, позволяющие достигнуть глубоких и наиболее влажных слоев земли, обладающих наибольшей проводимостью и не подвергающихся высыханию или промерзанию. Однако здесь необходимо учитывать, что с уменьшением сопротивления грунта возрастает коррозия металла. Кроме того, применение таких заземлителей не связано со значительными земляными работами, что неизбежно, например, при выполнении заземления из металлических листов или горизонтально закладываемых в землю металлических лент и проводов.

Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее (24 • 4) мм^2.

Проводник, соединяющий заземлитель с контуром заземления, должен быть луженым для уменьшения гальванической коррозии, а соединения должны быть защищены от воздействия влаги.

Магистрали заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания - по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Соединяют магистрали с заземлителем только с помощью сварки. К заземляемому устройству ТСПИ магистраль подключают с помощью болтового соединения в одной точке.

Для уменьшения сопротивлений контактов наилучшим является постоянное непосредственное соединение металла с металлом, полученное сваркой или пайкой. При соединении под винт необходимо применять шайбы (звездочки или Гровера), обеспечивающие постоянство плотности соединения.

При соприкосновении двух металлов в присутствии влаги возникает гальваническая и (или) электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага является электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду.

Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей.

Наиболее эффективным методом защиты от коррозии является применение металлов с малой электрохимической активностью, таких, как олово, свинец, медь. Значительно уменьшить коррозию и обеспечить хороший контакт можно, тщательно изолируя соединения от проникновения влаги.

5.3.3 Фильтрация информационных сигналов

Одним из методов **локализации опасных сигналов**, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства - источника опасного сигнала. Фильтрация в устройствах - рецепторах электромагнитных полей и наводок должна исключить их воздействие на рецептор.

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы.

Такие трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

- разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;
- устранения асимметричных наводок;
- ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (~10^4 МОм) и незначительной емкости между обмотками.

Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на выходе трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

Помехоподавляющие фильтры

В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т.д. Основное назначение фильтров - пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются **фильтры нижних частот.**

Фильтр нижних частот **(ФНЧ)** пропускает сигналы с частотами ниже граничной частоты ($f \leq f_{гр}$) и подавляет- с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L.

Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость С.

Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т.д.) конструируют на основе сочетаний различных единичных звеньев.

Количественно величина ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением:

$$A = 20\lg\left(\frac{U_1}{U_2}\right) = 10 \cdot \lg\left(\frac{P_1}{P_2}\right), \text{ дБ},$$

где U_1 (P_1) - напряжение (мощность) опасного сигнала на входе фильтра;

U_2 (P_2) - напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке $Z_Н$.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
- габариты и масса фильтров должны быть минимальными;
- фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.);
- конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

- затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);
- сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;
- ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Рассмотрим влияние этих параметров более подробно.

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания, но не более их.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это может привести к тому, что:

- ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр;

- возникает взаимозависимость переходных процессов в различных нагрузках цепи питания.

Наибольшие скачки напряжения при этом возникают во время отключения нагрузок, так как большинство из них имеет индуктивный характер.

Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, а LC-фильтр из десяти или более элементов - более 200 дБ/декада.

Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40 ... 60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать экранированные фильтры с разъемами и использовать для соединения экранированные провода.

Фильтры с гарантируемым затуханием 100 дБ выполняют в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей.

Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (f_C) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад.

Ориентировочные значения максимального затухания для сетевых фильтров, приведены в табл. 5.11.

Таблица 5.11 - Значения максимального затухания для сетевых фильтров

Диапазон частот	Максимальное затухание фильтра вне полосы пропускания, дБ		
	экранированный		неэкранированный
	с разъемами	без разъемов	
Фильтры в цепях питания на токи не более 10 А			
$f_c \le f \le 10 f_c$	80	—	—
$10f_c \le f \le 100 f_c$	80	—	—
$f > 100 f_c$	70	—	—
Фильтры в цепях питания на токи более 1 0 А			
$f_c \le f \le 10 f_c$;	100	—	—

$10f_c \le f \le 100\ f_c$	100	—	—
$f > 100\ f_c$	90	—	—

Конструктивно фильтры подразделяются на:

- фильтры на элементах с сосредоточенными параметрами (LC-фильтры) - обычно предназначены для работы на частотах до 300 МГц;
- фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) - применяются на частотах свыше 1 ГГц;
- комбинированные - применяются на частотах 300 МГц ... 1 ГГц.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров (ФП, ФБ, ФПС и др.). На рис. 4.8 ... 4.10 представлены принципиальные электрические схемы фильтров типа ФП, обеспечивающих эффективность фильтрации не менее 60 дБ, 80 дБ и 100 дБ соответственно.

Фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток - от 2,5 до 70 А. Размеры фильтров составляют от 350•100•60 до 560•210•80 мм, а вес - от 2,5 до 25 кг.

Фильтры серии ФСПК-100 (200) предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ.

Конструктивно фильтры ФСПК выполнены в виде двух корпусов (полукомплектов), каждый из которых обеспечивает фильтрацию двухпроводной линии. Размеры одного корпуса составляют 800•320•92 мм, а вес- 18кг.

5.3.4 Пространственное и линейное зашумление

Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ТСПИ и тем самым к уменьшению отношения опасный сигнал/шум (с/ш). Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

Для исключения **перехвата побочных электромагнитных излучений** по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС- линейное зашумление.

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

- система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

- создаваемые помехи не должны иметь регулярной структуры;
- уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);
- на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по ЭМС.

Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ.

В системах пространственного зашумления в основном используются помехи типа **"белого шума"** или **"синфазные помехи".**

Системы, реализующие метод "синфазной помехи", в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует "имитационную помеху", по спектральному составу соответствующую скрываемому сигналу.

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

Генераторы шума выполняются или в виде отдельного блока с питанием от сети 220В ("Гном", "Волна", "ГШ-1000" и др.), или в виде отдельной платы, вставляемой (встраиваемой) в свободный слот системного блока ПЭВМ и питанием от общей шины компьютера ("ГШ-К-1000", "Смог" и др.).

Генераторы, выполненные в виде отдельного блока, имеют сравнительно небольшие размеры и вес. Например, генератор шума "Гном-3" при размерах 307о95о49 мм весит 1,8 кг.

Диапазон рабочих частот генераторов шума от 0,01 ... 0,1 до 1000 МГц. При мощности излучения около 20 Вт обеспечивается спектральная плотность помехи 40 ... 80 дБ.

В системах пространственного зашумления в основном используются слабонаправленные рамочные жесткие и гибкие антенны. Рамочные гибкие антенны выполняются из обычного провода и разворачиваются в двух-трех плоскостях, что

обеспечивает формирование помехового сигнала как с вертикальной, так и с горизонтальной поляризацией во всех плоскостях.

При использовании систем пространственного зашумления необходимо помнить, что наряду с помехами средствам разведки создаются помехи и другим радиоэлектронным средствам (например, системам телевидения, радиосвязи и т.д.). Поэтому при вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости (ЭМС). Кроме того, уровни помех, создаваемые системой зашумления, должны соответствовать санитарно-гигиеническим нормам. Однако нормы на уровни электромагнитных излучений по требованиям ЭМС существенно строже санитарно-гигиенических норм. Следовательно, основное внимание необходимо уделять выполнению норм ЭМС.

Пространственное зашумление эффективно не только для закрытия электромагнитного, но и электрического каналов утечки информации, так как помеховый сигнал при излучении наводится в соединительных линиях ВТСС и посторонних проводниках, выходящих за пределы контролируемой зоны.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны. Они используются в том случае, если не обеспечивается требуемый разнос этих проводников и ТСПИ (то есть не выполняется требование по Зоне № 1), однако при этом обеспечивается требование по Зоне № 2 (то есть расстояние от ТСПИ до границы контролируемой зоны больше, чем Зона № 2).

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник). На практике наиболее часто подобные системы используются для зашумления линий электропитания (например, линий электропитания осветительной и розеточной сетей).

Глава 6. Методы и средства поиска электронных устройств перехвата информации

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 и**нформативными 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.

Классификация методов и средств поиска электронных устройств перехвата информации

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры: детекторов диктофонов и видеокамер, индикаторов поля, радиочастотомеров и интерсепторов, сканерных приемников и анализаторов спектра, программно-аппаратных комплексов контроля, нелинейных локаторов, рентгеновских комплексов, обычных тестеров, а также специальной аппаратуры для проверки проводных линий и т.д.

Метод поиска закладных устройств во многом определяется использованием той или иной аппаратуры контроля.

К основным методам поиска закладных устройств можно отнести:

- специальное обследование выделенных помещений;
- поиск радиозакладок с использованием индикаторов поля, радиочастотомеров и интерсепторов;
- поиск радиозакладок с использованием сканерных приемников и анализаторов спектра;
- поиск радиозакладок с использованием программно-аппаратных комплексов контроля;
- поиск портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- поиск портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию побочных электромагнитных излучений генераторов подмагничивания и электродвигателей видеокамер);
- поиск закладок с использованием нелинейных локаторов;
- поиск закладок с использованием рентгеновских комплексов;
- проверка с использованием ВЧ-пробника (зонда) линий электропитания, радиотрансляции и телефонной связи;
- измерение параметров линий электропитания, телефонных линий связи и т.д.;
- проведение тестового "прозвона" всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Простейшими и наиболее дешевыми обнаружителями радиоизлучений закладных устройств являются индикаторы электромагнитного поля, которые световым или

звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с напряженностью выше пороговой (фоновой). Более сложные из них - частотомеры обеспечивают, кроме того, измерение несущей частоты наиболее "сильного" в точке приема сигнала.

Для обнаружения излучений закладных устройств в ближней зоне могут использоваться и специальные приборы, называемые интерсепторами. Интерсептор автоматически настраивается на частоту наиболее мощного сигнала и осуществляет его детектирование. Некоторые интерсепторы позволяют не только производить автоматический или ручной захват радиосигнала, осуществлять его детектирование и прослушивание через динамик, но и определять частоту обнаруженного сигнала и вид модуляции.

Чувствительность обнаружителей поля мала, поэтому они позволяют обнаруживать излучения радиозакладок в непосредственной близости от них.

Существенно лучшую чувствительность имеют специальные (профессиональные) радиоприемники с автоматизированным сканированием радиодиапазона (сканерные приемники или сканеры). Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок - от десятков кГц до единиц ГТц. Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра. Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнаружении радиозакладок, использующих для передачи информации сложные виды сигналов.

Возможность сопряжения сканирующих приемников с переносными компьютерами послужило основой для создания автоматизированных комплексов для поиска радиозакладок (так называемых программно-аппаратных комплексов контроля). Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладных устройств используются и специально разработанные многофункциональные комплексы, такие, например, как **"OSCOR-5000".**

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Обнаружители пустот позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройствах, электропроводящие металлические детали конструкции и т.д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам - нелинейные радиолокаторы.

Принципы работы **нелинейных радиолокаторов** близки к принципам работы радиолокационных станций, широко применяемых для радиолокационной разведки

объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Металлоискатели (металлодетекторы) реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные рентгеновские установки применяются для просвечивания предметов, назначения которых не удается выявить без их разборки прежде всего тогда, когда она невозможна без разрушения найденного предмета.

Глава 7. Организация инженерно-технической защиты информации

7.1 Общие положения по инженерно-технической защите информации в организациях

Рассмотренные ранее вопросы создают теоретическую базу для построения, модификации и эксплуатации системы зашиты информации.

Любая система создается под заданные требования с учетом существующих ограничений. Факторы, влияющие на структуру и функционирование системы, называются системообразующими.

К ним относятся:

перечни защищаемых сведений, составляющих государственную (по тематике государственного заказа, если он выполняется организацией) и коммерческую тайну:

- требуемые уровни безопасности информации, обеспечение которых не приведет к превышению ущерба над затратами на защиту информации;
- угрозы безопасности информации;
- ограничения, которые надо учитывать при создании или модернизации системы защиты информации;
- показатели, по которым будет оцениваться эффективность системы защиты.

Структура и алгоритм функционирования системы защиты организации определяются в руководящих, нормативных и методических документах.

К руководящим документам относятся:

- руководство (инструкция) по защите информации в организации;
- положение о подразделении организации, на которое возлагаются задачи по обеспечению безопасности информации;
- инструкции по работе с грифованными документами;
- инструкции по защите информации о конкретных изделиях;

В различных организациях эти документы могут иметь разные наименования, отличающиеся от указанных. Но сущность этих документов остается неизменной, так как необходимость в них объективна.

Порядок защиты информации в организации определяется соответствующим руководством (инструкцией). Оно может содержать следующие разделы :

- общие положения;
- перечень охраняемых сведений;
- демаскирующие признаки объектов организации;
- демаскирующие вещества, создаваемые в организации;
- оценки возможностей органов и средств добывания информации;
- организационные и технические мероприятия по защите информации;
- порядок планирования работ службы безопасности;
- порядок взаимодействия с государственными органами, решающими задачи по защите материальной и интеллектуальной собственности, государственной и коммерческой тайны.

Но в данном руководстве нельзя учесть всех особенностей защиты информации в конкретных условиях. В любой организации постоянно меняется ситуация с источниками и носителями конфиденциальной информации, угрозами ее безопасности. Например, появлению нового товара на рынке предшествует большая работа, включающая различные этапы и стадии: проведение исследований, разработка лабораторных и действующих макетов, создание опытного образца и его доработка по результатам испытаний, подготовка производства (документации, установка дополнительного оборудования, изготовление оснастки - специфических средств производства, необходимых для реализации технологических процессов), изготовление опытной серии для выявления спроса на товар, массовый выпуск продукции.

На каждом этапе и стадии к работе подключаются новые люди, разрабатываются новые документы, создаются узлы и блоки с информативными для них демаскирующими признаками. Созданию каждого изделия или самостоятельного документа сопутствует свой набор информационных элементов, их источников и носителей, угроз и каналов утечки информации, проявляющиеся в различные моменты времени.

Для защиты информации об изделии на каждом этапе его создания разрабатывается соответствующая инструкция. Инструкция должна содержать необходимые для обеспечения безопасности информации сведения, в том числе: общие сведения о наименовании образца, защищаемые сведения и демаскирующие признаки, потенциальные угрозы безопасности информации, замысел и меры по защите, порядок контроля (задачи, органы контроля, имеющие право на проверку, средства контроля, допустимые значения контролируемых параметров, условия и методики, периодичность и виды контроля), фамилии лиц, ответственных за безопасность информации.

Основным нормативным документом является перечень сведений, составляющих государственную, военную, коммерческую или любую другую тайну. Перечень сведений, содержащих государственную тайну, основывается на положениях закона «О государственной тайне». Перечни подлежащих защите сведений этого закона конкретизируются ведомствами применительно к тематике конкретных организаций. В коммерческих структурах, выполняющих государственные заказы, перечни распространяются на информацию, относящуюся к этому заказу. Перечни сведений,

составляющих коммерческую тайну, составляются руководством фирмы при участии сотрудников службы безопасности.

Другие нормативные документы определяют максимально допустимые значения уровней полей с информацией и концентрации демаскирующих веществ на границах контролируемой зоны, которые обеспечивают требуемый уровень безопасности информации. Эти нормы разрабатываются соответствующими ведомствами, а для коммерческих структур, выполняющих негосударственные заказы, - специалистами этих структур.

Работа по защите информации в организации проводится всеми его сотрудниками, но степень участия различных категорий существенно отличается. Любой сотрудник, подписавший обязательство о неразглашении тайны, участвует в защите информации хотя бы путем выполнения руководящих документов о защите информации.

Ответственность за состояние защиты информации возлагается на соответствующее подразделение и лиц службы безопасности. Применительно к типовой структуре службы безопасности коммерческой структуры инженерно-техническая защита обеспечивается группой инженерно-технической защиты, которая, как вариант, может состоять из старшего инженера (инженера) - руководителя группы и инженера (техника) по специальным измерениям.

Основные задачи группы:

- обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации черезтехнические средства, конструкции зданий и оборудования;
- выявление и оценка степени опасности технических каналов утечки информации;
- разработка мероприятий по ликвидации (предотвращению утечки) потенциальных каналов утечки информации:
- организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий, анализ результатов контроля и разработка предложений по повышению надежности и эффективности мер зашиты;
- подготовка заявок на приобретение технических средств защиты информации, участие в их установке, эксплуатации и контроле состояния.

Кроме того, на группу инженерно-технической защиты информации целесообразно возложить также технические вопросы охраны носителей информации.

Организационные и технические меры по инженерно-технической защите информации

В организациях работа по инженерно-технической защите информации включает два этапа:

- построение или модернизация системы защиты;
- поддержание защиты информации на требуемом уровне.

Построение системы защиты информации проводится во вновь создаваемых организациях, в остальных - модернизация существующей. Методические вопросы построения и модернизации системы защиты информации рассмотрены в следующей главе

Построение (модернизация) системы защиты информации и поддержание на требуемом уровне ее защиты в организации предусматривают проведение следующих основных работ:

- уточнение перечня защищаемых сведений в организации, определение источников и носителей информации, выявление и оценка угрозы ее безопасности;
- определение мер по защите информации, вызванных изменениями целей и задач защиты, перечня защищаемых сведений, угроз безопасности информации;
- контроль эффективности мер по инженерно-технической защите информации в организации.

Меры по защите информации целесообразно разделить на 2 группы: организационные и технические. В публикациях, в том числе в некоторых руководящих документах, меры по защите делят на организационные, организационно-технические и технические. Учитывая отсутствие достаточно четкой границы между организационно-техническими и организационными, организационно-техническими и техническими мерами, целесообразно ограничиться двумя группами: организационными и техническими. При такой классификации к техническим относятся меры, реализуемые путем установки новых или модернизации используемых инженерных и технических средств защиты информации. Основу организационных мер инженерно-технической защиты информации составляют меры, определяющие порядок использования этих средств.

Организационные меры инженерно-технической зашиты информации включают, прежде всего, мероприятия по эффективному использованию технических средств регламентации и управления доступом к защищаемой информации, а также по порядку и режимам работы технических средств защиты информации. Организационные меры инженерно-технической защиты информации являются частью ее организационной зашиты, основу которой составляют регламентация и управление доступом.

Регламентация - это установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленные на обеспечение безопасности информации.

Регламентация предусматривает:

- установление границ контролируемых и охраняемых зон;
- определение уровней защиты информации в зонах;
- регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т. д.);
- определение режимов работы технических средств, в том числе сбора, обработки и хранения защищаемой информации на ПЭВМ, передачи документов, порядка складирования продукции и т. д.

Управление доступом к информации включает следующие мероприятия:

- идентификацию лиц и обращений

- проверку полномочий лиц и обращений;
- регистрацию обращений к защищаемой информации;
- реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений по каналам телекоммуникаций проводится с целью их надежного опознавания. Способы идентификации рассмотрены выше.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

Реагирование на любое обращение к информации заключается либо в разрешении доступа к информации, либо в отказе. Отказ может сопровождаться включением сигнализации, оповещением службы безопасности или правоохранительных органов, задержанием злоумышленника при его попытке несанкционированного доступа к защищаемой информации.

Технические меры предусматривают применение способов и средств, рассмотренных в данной книге.

Важнейшее и необходимое направление работ по защите информации – контроль эффективности зашиты. Этот вид деятельности проводится, прежде всего, силами службы безопасности, а также руководителями структурных подразделений. Контроль инженерно-технической защиты является составной частью контроля защиты информации в организации и заключается, прежде всего, в определении (измерении) показателей эффективности зашиты техническими средствами и сравнении их с нормативными.

Применяют следующие виды контроля:

1. предварительный;
2. периодический;
3. постоянный.

Предварительный контроль проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в том числе:

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

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

Наиболее часто должен проводиться периодический контроль на химических предприятиях, так как незначительные нарушения в технологическом процессе могут привести к утечке демаскирующих веществ. Для определения концентрации демаскирующих веществ регулярно берутся возле предприятия пробы воздуха, воды, почвы, снега, растительности.

Периодичность и места взятия проб определяются характером производства с учетом условий возможного распространения демаскирующих веществ, например, розы ветров и скорости воздушных потоков, видов водоемов (искусственный, озеро, болото, река и др.), характера окружающей местности и т. д. Пробы воздуха рекомендуется брать с учетом направлений ветра на высоте примерно 1.5 м в непосредственной близости от границ территории (50-100 м) и в зоне максимальной концентрации демаскирующих веществ, выбрасываемых в атмосферу через трубы. Пробы воды берутся в местах слива в водоемы в поверхностном слое и на глубине 30-50 см с последующим смешиванием. Берутся также пробы почвы и пыли на растительности. С этой целью собирают листья с нескольких деревьев и кустов на уровне 1.5-2 м от поверхности и не ранее недели после дождя.

Периодический (ежедневный, еженедельный, ежемесячный) контроль должен проводится также сотрудниками организации в части источников информации, с которыми они работают.

Общий (в рамках всей организации) периодический контроль проводится обычно 2 раза в год. Целью его является тщательная проверка работоспособности всех элементов и системы защиты информации в целом.

Постоянный контроль осуществляется выборочно силами службы безопасности и привлекаемых сотрудников организации с целью объективной оценки уровня защиты информации и. прежде всего, выявления слабых мест в системе защиты организации. Кроме того, такой контроль оказывает психологическое воздействие на сотрудников организации, вынуждая их более тщательно выполнять требования по обеспечению защиты информации.

Меры контроля, также как и защиты, представляют совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по защите информации. Организационные меры контроля включают:

- проверку выполнения сотрудниками требований руководящих документов по защите информации;
- проверку работоспособности средств охраны и защиты информации от наблюдения, подслушивания, перехвата и утечки информации по материально-вещественному каналу (наличие занавесок, штор, жалюзей на окнах, чехлов на разрабатываемых изделиях, состояние звукоизоляции, экранов, средств подавления опасных сигналов и зашумления, емкостейдля сбора отходов с демаскирующими веществами и т. д.);
- контроль за выполнением инструкций по защите информации о разрабатываемой продукции;
- оценка эффективности применяемых способов и средств защиты информации.

Технические меры контроля проводятся с использованием технических средств радио- и электроизмерений, физического и химического анализа и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемых зон;
- уровней опасных сигналов и помех в проводах и экранах кабелей, выходящих за пределы контролируемой зоны;
- степени зашумления генераторами помех структурных звуков в ограждениях;
- концентрации демаскирующих веществ в отходах производства.

Для измерения напряженности электрических полей используются селективные вольтметры/анализаторы спектра, панорамные приемники.

Следует также отметить, что добросовестное и постоянное выполнение сотрудниками организации требований по защите информации основывается на рациональном сочетании способов принуждения и побуждения.

Принуждение - способ, при котором сотрудники организации вынуждены соблюдать правила обращения с источниками и носителями конфиденциальной информации под угрозой материальной, административной или уголовной ответственности.

Побуждение предусматривает использование для создания у сотрудников установки на осознанное выполнение требований по защите информации, формирование моральных, этических, психологических и других нравственных мотивов. Воспитание побудительных мотивов у сотрудников организации является одной из задач службы безопасности, но ее усилия найдут благодатную почву у тех сотрудников, которые доброжелательно относятся к руководству организации и рассматривают организацию как долговременное место работы. Создание условий, при которых место работы воспринимается как второй дом, является, по мнению компетентных аналитиков, одним из факторов экономического роста Японии. Поэтому эффективность защиты в значительной степени влияет климат в организации, который формируется ее руководством.

Глава 8. Методическое обеспечение инженерно-технической защиты информации

8.1 Системный подход к защите информации

В общем случае способы и средства технической защиты информации должны создать вокруг объекта защиты преграды, препятствующие реализации угроз безопасности информации как при непосредственном контакте злоумышленников с ее источниками, так и при ее утечке. Учитывая активность, непрерывность, скрытность разведки, большое количество потенциальных источников информации в организациях, многообразие побочных полей и электрических сигналов, возникающих при обработке, хранении и передаче информации и способных уносить ее за пределы объекта защиты, проблема защиты информации относится к числу сложных, так называемых слабоформализуемых проблем. Эти проблемы не имеют, как правило, формальных методов решения.

Слабо формализуемые проблемы и задачи наиболее часто приходится решать как коллективам, так и отдельным людям. Несмотря на огромные достижения науки число проблем и задач, которые удается свести к формализуемым и решить строго математически, существенно меньше, чем не имеющих такого решения.

В общем случае рассматриваемые проблемы и задачи характеризуются большим количеством и многообразием факторов, влияющих на результат решения, причем это влияние часто не удается однозначно выявить и строго описать. К ним. в первую очередь,

относятся задачи, результаты решения которых зависят от людей. Только в отдельных простейших случаях удается однозначно и формально описать реакции человека на внешние воздействия. В большинстве других вариантов сделать это не удается.

Однако из этого утверждения не следует, что организация эффективной защиты информации зависит исключительно от искусства специалистов по защите информации. Человечеством накоплен достаточно большой опыт по решению слабоформализуемых проблем, который оформлен как системный подход к решению слабоформализуемых проблем и системный анализ объектов исследования.

Системный подход - это концепция решения сложных слабоформализуемых проблем, рассматривающая объект изучения (исследования) или проектирования в виде системы.

Основные принципы системного подхода состоят в следующем:

- любая система является подсистемой более сложной системы, которая влияет на структуру и функционирование рассматриваемой;
- любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных оснований;
- при анализе системы необходим учет внешних и внутренних влияющих факторов, принятие решений на основе их небольшого числа без рассмотрения остальных может привести к нереальным результатам;
- накопление и объединение свойств элементов системы приводит к появлению качественно новых свойств, отсутствующих у ее элементов.

Последний принцип утверждает, что система как целое приобретает дополнительные свойства, отсутствующие у ее частей, в отличие от традиционного, который предполагает, что свойства объекта или субъекта есть совокупность свойств его частей. Примером традиционного подхода могут служить используемые официальной медициной методы диагностики и лечения болезней человека по результатам исследования отдельных его органов. Человек к старости после прохождения многочисленных кабинетов узкоспециализированных врачей приобретает такой букет болезней, что если он будет строго выполнять все рекомендации врачей, то ему грозит отравление лекарствами гораздо раньше срока естественной смерти. В то же время результаты исследований доказывают, что человека нельзя делить на части без учета информационных, химических, электромагнитных, электрических связей между его органами и даже клетками и что лечить надо не отдельные болезни, а человека в целом. Пренебрежение принципом целостности в медицине привело к тому, что образовавшуюся нишу заполняют знахари, экстрасенсы, так называемые народные целители и другие «самородки», заряжающие энергией зубные пасты и газеты.

Эффективность реализации системного подхода на практике зависит от умения специалиста выявлять и объективно анализировать все многообразие факторов и связей достаточно сложного объекта исследования, каким является, например, организация как объект защиты. Необходимым условием такого умения является наличие у специалиста так называемого системного мышления, формируемого в результате соответствующего обучения и практики решения слабоформализуемых проблем. Системное мышление - важнейшее качество не только специалиста по защите информации, но любою организатора и руководителя.

Системный анализ предусматривает применение комплекса методов, методик и процедур, позволяющих выработать количественные рекомендации по решению любых, прежде всего, слабоформализуемых проблем. Математической основой для системного анализа является аппарат исследования операций.

С позиции системного подхода совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности информации, образует систему зашиты информации. Такими элементами являются люди (руководство и сотрудники организации, прежде всего, службы безопасности), инженерные конструкции и технические средства, обеспечивающие защиту информации. Следует подчеркнуть, что речь идет не о простом наборе взаимосвязанных элементов, а объединенных целями и решаемыми задачами.

Система задается (описывается) следующими параметрами (характеристиками):

- целями и задачами (конкретизированными в пространстве и во времени целями);
- входами и выходами системы;
- ограничениями, которые необходимо учитывать при построении (модернизации, оптимизации) системы;
- процессами внутри системы, обеспечивающими преобразование входов в выходы.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы в требуемую.

Целями системы защиты являются обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (в общем случае - на объекте защиты). Задачи конкретизируют цели применительно к видам и категориям защищаемой информации, а также элементам объекта защиты и отвечают на вопрос, что надо сделать для достижения целей. Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использования ее злоумышленником во вред владельцу информации.

Рис. 8.1. Основные характеристики системы зашиты

В качестве ориентира для оценки требуемого уровня защиты необходимо определить соотношение между ценой защищаемой информации и затратами на ее защиту. Уровень защиты рационален, когда обеспечивается требуемый уровень безопасности информации и минимизируются расходы на информацию. Эти расходы Сри складываются из:

- затрат на защиту информации Сзи;

- ущерба Суи за счет попадания информации к злоумышленнику и использования ее во вред владельцу.

Между этими слагаемыми существует достаточно сложная связь, так как ущерб из-за недостаточной безопасности информации уменьшается с увеличением расходов на ее защиту.

Если первое слагаемое может быть точно определено, то оценка ущерба в условиях скрытности разведки и неопределенности прогноза использования злоумышленником полученной информации представляет достаточно сложную задачу. Ориентировочная оценка ущерба возможна при следующих допущениях.

Владелец информации ожидает получить от ее материализации определенную прибыль, которой он может лишиться в случае попадания ее конкуренту. Кроме того, последний, используя информацию, может нанести владельцу еще дополнительный ущерб за счет, например, изменения тактики, продажи или покупки ценных бумаг и т. д. Дополнительные неблагоприятные факторы чрезвычайно трудно поддаются учету. Поэтому в качестве граничной меры для оценки ущерба можно использовать величину потенциальной прибыли Спи, которую ожидает получить от информации ее владелец, т. е.

$$Суи \geq Спи$$

В свою очередь величина ущерба зависит от уровня защиты, определяемой расходами на нее. Максимальный ущерб возможен при нулевых расходах на защиту, гипотетический нулевой обеспечивается при идеальной защите. Но идеальная защита требует бесконечно больших затрат.

При увеличении расходов вероятность попадания информации злоумышленнику, а. следовательно, и ущерб уменьшаются. Но одновременно увеличиваются расходы на защиту. Указанные зависимости иллюстрируются на рис. 8.2.

Рис. 8 2. Зависимость расходов на информацию от затрат на ее защиту

Из рисунка следует, что функция Сри = f (Суи, Сзи) имеет область, в которой Сри принимает максимальное и минимальное значения. Рост суммарных расходов на информацию с увеличением затрат на ее защиту имеет место в период создания или модернизации системы, когда происходит накопление мер и средств защиты, которые еще не оказывают существенного влияния на безопасность информации. Например, предотвращение утечки информации по отдельным каналам без снижения вероятности утечки по всем остальным не приводит к заметному повышению безопасности информации, хотя затраты на закрытие отдельных каналов могут быть весьма существенными. Образно говоря, для объекта защиты существует определенная

«критическая масса» затрат на защиту информации, при превышении которой эти затраты обеспечивают эффективную отдачу.

При некоторых рациональных затратах на защиту информации выше критических наблюдается минимум суммарных расходов на информацию. При затратах ниже рациональных увеличивается потенциальный ущерб за счет повышения вероятности попадания конфиденциальной информации к злоумышленнику, при более высоких затратах - увеличиваются прямые расходы на защиту.

Ограничения системы представляют собой выделяемые на защиту информации людские, материальные, финансовые ресурсы, а также ограничения в виде требований к системе. Суммарные ресурсы удобно выражать в денежном эквиваленте. Независимо от выделяемых на защиту информации ресурсов они не должны превышать суммарной цены защищаемой информации. Это верхний порог ресурсов.

Ограничения в виде требований к системе предусматривают принятие таких мер по защите информации, которые не снижают эффективность функционирования системы при их выполнении. Например, можно настолько ужесточить организационные меры управления доступом к источникам информации, что наряду со снижением возможности ее хищения или утечки ухудшатся условия выполнения сотрудниками своих функциональных обязанностей.

Входами системы инженерно-технической защиты информации являются:

- воздействия злоумышленников при физическом проникновении к источникам конфиденциальной информации с целью ее хищения, изменения или уничтожения;
- различные физические поля электрические сигналы, создаваемые техническими средствами злоумышленников и которые воздействуют на средства обработки и хранения информации;
- стихийные силы, прежде всего, пожара, приводящие к уничтожению или изменению информации;
- физические поля и электрические сигналы с информацией, передаваемой по функциональным каналам связи;
- побочные электромагнитные и акустические поля, а также электрические сигналы, возникающие в процессе деятельности объектов защиты и несущие конфиденциальную информацию.

Выходами системы защиты являются меры по защите информации, соответствующие входным воздействиям.

Алгоритм процесса преобразования входных воздействий (угроз) в меры защиты определяет вариант системы защиты. Вариантов, удовлетворяющих целям и задачам, может быть много. Сравнение вариантов производится по количественной мере, называемой критерием эффективности системы. Критерий может быть в виде одного показателя, учитывающего основные характеристики системы или представлять собой набор частных показателе. Единый общий критерий эффективности называется глобальным.

В качестве частных показателей критерия эффективности системы защиты информации используются, в основном, те же, что и при оценке эффективности разведки. Это возможно потому, что цели и задачи, а, следовательно, значения показателей

эффективности разведки и защиты информации близки по содержанию, но противоположны по результатам. То, что хорошо для безопасности информации, плохо для разведки, и наоборот.

Частными показателями эффективности системы защиты информации являются:

- вероятность обнаружения и распознавания органами разведки объектов защиты;
- погрешности измерения признаков объектов зашиты;
- качество (разборчивость) речи на выходе приемника злоумышленника;
- достоверность (вероятность ошибки) дискретного элемента информации (буквы, цифры, элемента изображения).

Очевидно, что система зашиты тем эффективнее, чем меньше вероятность обнаружения и распознавания объекта защиты органом разведки (злоумышленником), чем ниже точность измерения им признаков объектов защиты, ниже разборчивость речи, выше вероятность ошибки приема органом разведки дискретных сообщений.

Однако при сравнении вариантов построения системы по нескольким частным показателям возникают проблемы, обусловленные возможным противоположным характером изменения значений разных показателей: одни показатели эффективности одного варианта могут превышать значения аналогичных показателей второго варианта, другие наоборот - имеют меньшие значения. Какой вариант предпочтительнее? Кроме того, важным показателем системы зашиты являются затраты на обеспечение требуемых значений оперативных показателей. Поэтому результаты оценки эффективности защиты по совокупности частных показателей, как правило, неоднозначные.

Для выбора рационального (обеспечивающего достижение целей, решающего поставленные задачи при полном наборе входных воздействий с учетом ограничении) варианта путем сравнения показателей нескольких вариантов используется глобальный критерий в виде отношения эффективность/стоимость. Под эффективностью понимается степень выполнения системой задач, под стоимостью - затраты на защиту.

В качестве меры эффективности $К_э$ применяются различные композиции частных показателей, чаще их «взвешенная» сумма:

$$К_э = \sum_{i=1}^{n} \alpha_i \mathbf{К}_i ,$$

где α_i- «вес» частного показателя эффективности $К_i$.

«Вес» частного показателя определяется экспертами (руководством, специалистами организации, сотрудниками службы безопасности) в зависимости от характера защищаемой информации. Если защищается в основном семантическая информация, то больший «вес» имеют показатели оценки разборчивости речи и вероятности ошибки приема дискретных сообщений. В случае защиты объектов наблюдения выше «вес» показателей, характеризующих вероятности обнаружения и распознавания этих объектов.

Для оценки эффективности системы защиты информации по указанной формуле частные показатели должны иметь одинаковую направленность влияния на эффективность -

при увеличении их значений повышается значение эффективности. С учетом этого требования в качестве меры обнаружения и распознавания объекта надо использовать вероятность не обнаружения и не распознания, а вместо меры качества подслушиваемой речи - ее неразборчивость. Остальные частные показатели соответствуют приведенным выше. Выбор лучшего варианта производится по максимуму глобального критерия, так как он имеет в этом случае лучшее соотношение эффективности и стоимости.

Проектирование требуемой системы защиты проводится путем системного анализа существующей и разработки вариантов требуемой. Алгоритм этого процесса включает следующие этапы:

- определение перечня защищаемой информации, целей, задач, ограничений и показателей эффективности системы зашиты;
- моделирование существующей системы и выявление ее недостатков с позиции поставленных целей и задач;
- определение и моделирование угроз безопасности информации;
- разработка вариантов (алгоритмов функционирования) проектируемой системы;
- сравнение вариантов по глобальному критерию и частным показателям, выбор наилучших вариантов:
- обоснование выбранных вариантов системы в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы защиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате нескольких итераций.

Алгоритм проектирования системы зашиты информации представлен на рис. 8.3.

В ходе проектирования создаются модели объектов зашиты и угроз безопасности информации, в том числе модели каналов утечки информации, оцениваются угрозы, разрабатываются способы защиты информации, выбираются технические средства, определяются эффективность зашиты и необходимые затраты. Разработка способов и средств защиты информации прекращается, когда достигается требуемый уровень ее безопасности, а затраты на защиту соответствуют ресурсам.

После рассмотрения руководством предлагаемых вариантов (лучше двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы зашиты.

Следует подчеркнуть, что специалист по защите информации должен при обосновании предлагаемых руководству организации вариантов защиты учитывать психологию лица (руководителя), принимающего решение о реализации предложений, и в большинстве случаях недостаточную информированность его об угрозах безопасности информации в организации.

Психологическим фактором, сдерживающим принятие решения руководителем о выделении достаточно больших ресурсов на защиту информации является то

обстоятельство, что в условиях скрытности добывания информации угрозы ее безопасности не представляются достаточно серьезными, а приобретают некоторый абстрактный характер. Знание руководителем о существовании, в принципе, таких угроз, но без достаточно убедительных доводов специалиста о наличии угроз безопасности информации в конкретной организации, не гарантирует финансирование проекта в необходимом объеме. Кроме того, руководитель в силу собственного представления об угрозах, способах и средствах их нейтрализации может преувеличивать значимость одних мер защиты и преуменьшать другие. Однако это обстоятельство не должно уменьшать энтузиазм специалиста по защите информации, так как оно характерно для любого вида деятельности, а умение обосновывать свои предложения является необходимым качеством любого специалиста.

Рис. 8.3. Алгоритм проектирования системы защиты информации

Корректировка мер по защите информации производится после рассмотрения проекта руководством организации, а также в ходе реализации проекта и эксплуатации системы зашиты. Концепция системного подхода к обеспечению зашиты информации в США получила название «Opsec» (Operation Security). В соответствии с ней процесс организации защиты включает 7 этапов: от анализа объекта зашиты на первом этапе до доведения персоналу фирмы мер по безопасности информации и осуществления контроля.

Для зашиты информации на основе системного подхода и анализа необходимо, наряду с организационным и техническим, методическое обеспечение, В соответствии с алгоритмом проектирования системы оно должно обеспечивать:

- моделирование объекта защиты;
- выявление и моделирование угроз безопасности информации;
- разработку мер инженерно-технической защиты информации.

8.2 Моделирование объектов защиты

Моделирование объектов защиты включает:

- структурирование защищаемой информации;
- разработку моделей объектов защиты.

Для структурирования информации в качестве исходных данных используются:

- перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;
- перечень источников информации в организации. Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам. Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации разрабатывается в виде графа-структуры, нулевой (верхний) уровень иерархии которой соответствует понятию «защищаемая информация», а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации - общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация не должна указываться в разных элементах классификации.

Результаты структурирования оформляются в виде:

- схемы классификации информации;
- таблицы, вариант формы котором приведен в табл. 8.1.

Таблица разрабатывается на основе схемы классификации информации. В первом столбце указывается номер элемента информации в схеме классификации.

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации (рис. 1.2). Значимость номера равна количеству уровней структуры, а каждая цифра - порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня, который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-й темы 1-го уровня.

Таблица 8.1.

№ элемента информации	Наименование элемента информации	Гриф конфиденциальности информации	Цепа информа-ции	Наименование источника информаци	Местонахождение источника информации
1	2	3	4	5	6

Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. Последующие столбцы таблицы относятся к источникам информации соответствующего ее элемента в схеме классификации. В столбце 5 указывается наименование источника (фамилия человека, название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в графе 6 -места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Эти места в общем случае представляют собой:

- помещения (служебные, лаборатории, офисы, цеха, склады, квартиры и др);
- письменные столы рабочих мест сотрудников, хранилища и сейфы, шкафы деревянные и металлические в помещениях.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Основным методом исследования систем защиты является моделирование. Описание или физический аналог любого объекта, в том числе системы защиты информации и ее элементов, создаваемые для определения и исследования свойств объекта, представляют собой его модели. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта. Анализ (исследование) модели объекта называется моделированием. Различают вербальные, физические и математические модели и соответствующее моделирование.

Вербальная модель описывает модель на национальном и профессиональном языках. Человек постоянно создает вербальные модели окружающей его среды и руководствуется ими при принятии решений. Чем точнее модель отображает мир, тем эффективнее при прочих равных условиях деятельность человека. На способности разных людей к адекватному моделированию окружающего мира влияют как природные (генетические) данные, так и воспитание, обучение, в том числе на основе собственного опыта, физическое и психическое состояния человека, а также мировоззренческие модели общества, в котором живет конкретный человек.

В основе многих болезней психики человека лежат нарушения механизма моделирования окружающей среды. В крайних ее проявлениях в больном мозгу создаются модели, имеющие мало сходства с общепринятыми или объективно существующими моделями окружающего мира. В этом случае поступки больного человека на основе искаженной модели не соответствуют моделям других людей, а поведение такого человека классифицируется как ненормальное. Понятие «нормы» является достаточно условным и субъективным и может меняться в значительных пределах. Творческие люди способны в своем воображении создавать модели, отличающиеся от реальности, и эти модели в какой-то мере влияют на их поведение, которое иным людям кажется странным.

Так как основу жизни человека составляют химические и электрические процессы в его организме, то модели окружающей среды могут искажаться под действием химических наркотических веществ. Люди постоянно пользуются наркотиками, чтобы подкорректировать свои модели внешнего мира с целью уменьшить уровень отрицательных эмоций, возникающих при информационной недостаточности или несоответствия жизненных реалий задачам и целям человека. Наркотические вещества

(алкоголь, табак, кофеин, кола), вызывающие слабое наркотическое воздействие на организм человека, узаконены, другие (опиум, героин, ЛСД и т. д.) столь губительны, что наркомания рассматривается человечеством как одна из наиболее страшных угроз его существованию.

Физическая модель представляет материальный аналог реального объекта, которую можно подвергать в ходе анализа различным воздействиям, что часто трудно сделать по отношению к реальному объекту защиты.

Часто в качестве физических моделей исследуют уменьшенные копии крупных объектов, для изучения которых отсутствует инструментарий. Модели самолетов и автомобилей продувают в аэродинамических трубах, макеты домов испытывают на вибростендах и т. д.

По мере развития вычислительной математики и техники расширяется сфера применения математического моделирования на основе математического описания структуры и процессов в объекте, представляемом в виде системы. Математические модели могут разрабатываться в виде аналитических зависимостей выходов системы от входов, уравнений для моделирования динамических процессов в системе, статистических характеристик реакций системы на воздействия случайных факторов. Математическое моделирование позволяет наиболее экономно и глубоко исследовать сложные объекты, чего, в принципе, нельзя добиться с помощью вербального моделирования или чрезмерно дорого при физическом моделировании. Возможности математического моделирования ограничиваются уровнем формализации описания объекта и степенью адекватности математических выражений реальным процессам в моделируемом объекте.

Подобные ограничения возникают при моделировании сложных систем, элементами которых являются люди. Многообразие поведения конкретного человека пока не поддается описанию на языке математических символов. Однако в статистическом смысле поведение человека более прогнозируемое и устойчивое.

Для моделирования сложных систем все шире применяется метод математического моделирования, называемый имитационным моделированием. Оно предполагает определение реакций системы на внешние воздействия, которые генерирует ЭВМ в виде случайных чисел. Статистические характеристики (математическое ожидание, дисперсия, вид и параметры распределения) этих случайных чисел должны с приемлемой точностью соответствовать реальным воздействиям. Функционирование системы при случайных внешних воздействиях описывается в виде алгоритма действий элементов системы и их характеристик в ответ на каждое воздействие на входе. Таким образом имитируется работа сложной системы в сложных условиях. Путем статистической обработки выходных результатов при достаточно большой выборке входных воздействий получаются достоверные оценки работы системы. Например, достаточно объективная оценка эффективности системы защиты информации при многообразии действий злоумышленников, которые с точки зрения службы безопасности носят случайный характер, возможна, как правило, на основе имитационного моделирования системы защиты.

В чистом виде каждый вид моделирования используется редко. Как правило, применяются комбинации вербального, физического и математического моделирования. С вербального моделирования начинается сам процесс моделирования, так как нельзя создать физические или математические модели не имея образного представления об объекте и его словесного описания. Если есть возможность исследовать свойства объекта на

физической модели, то наиболее точные результаты обеспечиваются при физическом моделировании. Таким образом проверяют аэродинамику самолетов и автомобилей путем продувки уменьшенных физических моделей самолетов и автомобилей в аэродинамических трубах. Когда создание физической модели по тем или иным причинам невозможно или чрезмерно дорого, то проводят математическое моделирование, иногда дополняя его физическим моделированием отдельных узлов, деталей, т. е. тех частей объекта, описание которых не поддается формализации.

Так как создание и исследование универсальных (позволяющих проводить всесторонние исследования) моделей является достаточно дорогостоящим и трудным делом, то в целях упрощения моделей в них детализируют элементы и связи между ними, необходимые для решения конкретной поставленной задачи. Остальные, менее существенные для решения конкретной задачи элементы и связи укрупняют или не учитывают вовсе. В результате такого подхода экономным путем исследуются с помощью дифференцированных моделей отдельные, интересующие исследователя, свойства объекта Задача моделирования объектов зашиты состоит в объективном описании и анализе источников конфиденциальной информации и существующей системы ее защиты.

Моделирование объектов защиты включает:

- определение источников защищаемой информации;
- описание пространственного расположения основных мест размещения источников защищаемой информации;
- выявление путей распространения носителей с защищаемой информации за пределы контролируемых зон (помещений, зданий, территории организации);
- описание с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации - планов помещений, этажей зданий, территории в целом. На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Их параметры целесообразно объединить в таблице, вариант которой приведен в табл. 8.2.

Таблица 8.2.

1	Название помещения	
2	Этаж	Площадь, м"
3	Количество окон, тип сигнализа-ции, наличие штор на окнах	Куда выходят окна
4	Двери, кол-во, одинарные, двой-ные	Куда выходят двери

5	Соседние помещения, название, толщина стен	
6	Помещение над потолком/назва-ние, толщина перекрытии	
7	Помещение под полом, название, толщина перекрытии	
8	Вентиляционные отверстия, места размещения, размеры отверстий	
9	Батареи отопления, типы, куда выходя1 трубы	
10	Цепи электропитания	Напряжение. В. количество розеток электропитания, входящих и выходящих кабелей
11	Телефон	Типы, места установки телефонных аппаратов. тип кабеля
12	Радиотрансляция	Типы громкоговорителей места установки
13	Электрические часы	Тип, куда выходит кабель электрических часов
14	Бытовые радиосредства	Радиоприемники, телевизоры, аудио и видеомагнитофоны, их кол-во и типы
15	Бытовые электроприборы	Вентиляторы и др.. места их размещения
16	ПЭВМ	Кол-во, типы, состав, места размещения
17	Технические средства охраны	Типы и места установки извещателей, юны действий излучений
18	Телевизионные средства наблюдения	Места установки, типы и зоны наблюдения телевизионных трубок
19	Пожарная сигнализация	Типы извещателей, схемы соединения и вывода шлейфа
20	Другие средства	

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения и зоны наблюдения телевизионных камер и т. д.

На плане территории организации отмечаются места размещения здания (зданий), забора, КПП, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного

освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

Моделирование состоит в анализе на основе рассмотренных пространственных моделей возможных путей распространения информации за пределы контролируемой зоны и определении уровней полей и сигналов на их границах. Уровни полей и сигналов рассчитываются путем уменьшения мощностей на выходе источников сигналов, выраженных, например, в децибелах, на суммарную величину их ослабления в среде распространения к границам контролируемых зон.

В результате моделирования определяется состояние безопасности информации и слабые места существующей системы ее защиты. Результаты моделирования оформляются на планах и в таблицах.

8.3 Моделирование угроз безопасности информации

Моделирование угроз безопасности информации предусматривает анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба.

Моделирование угроз включает:

- моделирование способов физического проникновения злоумышленника к источникам информации;
- моделирование технических каналов утечки информации.

Действия злоумышленника по добыванию информации, так же как других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью. Так же как в криминалистике расследование преступления начинается с ответа на вопрос: кому это выгодно, так и прогноз способов физического проникновения следует начать с выяснения: кому нужна защищаемая информация. Способы проникновения исполнителей зарубежных спецслужб будут отличаться высокими квалификацией и технической оснащенностью, конкурентов - подготовленными исполнителями со средствами, имеющимися на рынке, криминальных структур - недостаточно подготовленными, но хорошо оснащенными исполнителями.

Для создания модели угрозы физического проникновения, достаточно близкой к реальной, необходимо «перевоплотиться» в злоумышленника, т. е. попытаться мысленно проиграть с позиции злоумышленника варианты проникновения к источнику информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели. В условиях отсутствия информации о злоумышленнике, его квалификации, технической оснащенности во избежания грубых ошибок лучше переоценить угрозу, чем ее недооценить, хотя такой подход и может привести к увеличению затрат на защиту.

На основе такого подхода модель злоумышленника выглядит следующим образом:

- злоумышленник представляет серьезного противника, тщательно готовящего операцию проникновения, изучает: обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) Освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

- имеет в распоряжении современные технические средства проникновения и преодоления механических преград;
- всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;
- проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

В зависимости от квалификации, способов подготовки и физического проникновения в организацию злоумышленников разделяют на следующие типы;

- неподготовленный, который ограничивается внешним осмотром объекта, проникает в организацию через двери и окна, при срабатывании тревожной сигнализации убегает;
- подготовленный, изучающий систему охраны объекта и готовящий несколько вариантов проникновения в организацию, в основном, путем взлома инженерных конструкций; - квалифицированный, который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы проникновения.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны.

Возможные пути проникновения злоумышленников отмечаются линиями на платах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в табл. 8.3.

Таблица 8.3.

№ элемента информации	Цена информации	Путь проникновения злоумышленника	Оценки реальности пути	Величина угрозы	Ранг угрозы
I	2	3	4	5	6

Обнаружение и распознавание каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить указанные в табл. 8. 4.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Таблица 8.4

Вид канала	Индикаторы
Оптический	Окна, выходящие на улицу, близость к ним противоположных домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзей. Просматриваемость содержания документов на столах со стороны окон, дверей, шкафов в помещении. Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей. Малое расстояние между столами сотрудников в помещении. Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей пли других сотрудников. Складирование продукции но дворе без навесов. Малая высота забора и дырки в нем. Переноска и перевозка образцов продукции в открытом виде. Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино и видеокамерами
Радио-электронный	Наличие в помещении радиоэлектронных средств. ПЭВМ. ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Выход окоп помещения на улицу, близость к ним улицы и противоположных домов Применение средств радиосвязи. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио и электрических приборов. Длительная и частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми.
Акустический	Малая толщина дверей и стен помещения Наличие в помещении открытых вентиляционный отверстии Отсутствие экранов на отопительных батареях Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей.
Материально-вещественный	Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничиваться одним или двумя. Например, от источника информации - руководителя фирмы утечка информации возможна по следующим каналам:

- через дверь в приемную или коридор;
- через окно на улицу или во двор;
- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения;
- по трубам отопления в другие помещения здания;

- через стены, потолок и пол в соседние помещения;
- с помощью закладных устройств за территорию фирмы.

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации, В основном применяются вербальные и математические модели. Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала канала является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;
- канал утечки включает разнообразные инженерные конструкции (бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздать которые на макетах невозможно или требуются огромные расходы.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют структурная и пространственная модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приемника сигналов, удаленность их от границ территории организации, ориентация вектора распространения носителя информации в канале утечки информации и его протяженность. Структурную модель канала целесообразно представлять в табличной форме, пространственную в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают функциональная и информационная модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержат характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и ее вид, источник сигнала, среда распространения и ее протяженность, место размещения приемника сигнала, информативность канала и величина угрозы безопасности информации.

Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале, позволяющих оценить максимальную дальность канала и показатели возможностей органов государственной и коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводится применительно к гипотетическому приемнику. В качестве приемника целесообразно рассматривать приемник, параметры которого соответствуют современному

уровню, а место размещения выбрано рационально. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует от крупных ошибок в значительно большей степени, чем пренебрежительное.

При описании приемника сигнала необходимо учитывать реальные возможности злоумышленника. Очевидно, что приемники сигналов коммерческой разведки не могут, например, размещаться на космических аппаратах. Что касается технических характеристик средств добывания, то они для государственной и коммерческой разведки существенно не отличаются. Расположение приемника злоумышленника можно приблизительно определить исходя из условий обеспечения значения отношения сигнал/помеха на входе приемника, необходимого для съема информации с допустимым качеством, и безопасности злоумышленника или его аппаратуры.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в табл. 8.5.

Наименование источника информации заимствуются из табл. 8.1. В графе 4 указываются основные элементы среды распространения и возможные места размещения приемника сигналов. По физической природе носителя определяется вид канала утечки информации.

Таблица 8.5.

№ элемента информации	Цена информации	Источник сигнала	Путь утечки информации	Вид канала	Оценки реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5	6	7	8

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

- добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации. Кроме того, следует иметь, что характер и частность реализации угроз зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах, например, в странах с развитой рыночной экономикой, не могут быть однозначно использованы для российских условий;
- оценка угроз безопасности информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях

острой информационной недостаточности;

- многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;
- априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику или ее утечки по техническому каналу проводятся с учетом меры (вероятности) $P_р$ реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации $С_и$.

Угроза безопасности информации, выраженной в величине ущерба $С_{уи}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала в виде $С_{уи} - С_и P_р$.

Моделирование угроз безопасности информации завершается их ранжированием в таблицах 8.4 и 8.5.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например, по виду, положению в пространстве, способам и средствам защиты, угрозам.

8.4 Методические рекомендации по разработке мер инженерно-технической защиты информации

Так как не существует формальных методов синтеза вариантов предотвращения угроз безопасности информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение, далее - с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит средств для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации. Перечень типовых способов и средств приведены в табл. 8. 6.

Таблица 8. 6.

Способы реализации угроз	Типовые способы и средства предотвращения угроз
Физический контакт злоумышленника с источником информации	Механические преграды (заборы. КПП. двери, взломостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз.
Воздействие огня	Технические средства пожарной сигнализации, средства пожаротушения, огнестойкие хранилища и сейфы.
Наблюдение	Маскировочное окрашивание, естественные и искусственные маски, ложные объекты, аэрозоли, пены, радиолокационные отражатели, радио- и звукопоглощающие покрытия, теплоизолирующие материалы, генераторы радио-и гидроакустических помех.
Подслушивание	Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие материалы, акустическое и вибрационное зашумление. обнаружение, изъятие и разрушение закладных устройств.
Перехват	Выполнение требований по регламент)' и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование, пространственное и линейное зашумление.
Утечка информации но материально-вещественному каналу	Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов.

Так как меры по защите информации рассматриваются для каждой угрозы, то в контролируемой зоне возможно их дублирование. Например, полуоткрытая дверь в служебное помещение может способствовать как наблюдению документов и экранов ПЭВМ в помещении, так и подслушиванию ведущихся в нем разговоров. Установленные на дверь устройство для автоматического ее закрытия и кодовый замок предотвращают утечку информации по этим каналам. После объединения способов и средств защиты информации освобожденные ресурсы могут быть использованы для предотвращения очередных по рангу угроз из табл. 8.3 и 8.5.

Следовательно, разработка мер по предотвращению угроз представляет собой итерационный процесс, каждая итерация которого выполняется в 2 этапа:

- разработка локальных мер по предотвращению каждой из выявленных угроз;
- интеграция (объединение) локальных мер.

Условием для перехода к следующей итерации является освобождение в результате объединения способов и средств защиты информации части ресурса, достаточной для предотвращения очередной угрозы.

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в табл. 8.7.

Таблица 8.7.

№ элемента информации	Тим угрозы	Величина угрозы	Способы предотвращен	Средства предотвраще	Затраты на предотвращения
1	2	3	4	5	6
Суммарные затраты на защиту информации					

Совокупность рассмотренных таблиц, планов и схем с результатами моделирования объектов защиты и угроз, а также предложений по способам и средствам защиты информации создают основу проекта по построению соответствующей системы или предложений по совершенствованию существующей системы.

В итоговой части проекта (служебной записке, предложениях) целесообразно оценить полноту выполнения задач по защите информации для выделенных ресурсов, а также нерешенные задачи и необходимые для их решения ресурсы.

Подготовленные документы (проект, служебная записка, предложения) предъявляются руководству для принятия решения. Наличие в них нескольких вариантов решений способствует более активному участию в построении или совершенствованию системы защиты информации руководителя организации в качестве как наиболее опытного и квалифицированного специалиста, так и распорядителя ресурсов организации.

После принятия проекта (предложений) начинается этап их реализации. Основные задачи специалистов по защите информации заключаются в контроле за работами по выполнению организационных и технических мероприятий, участие в приемке результатов работ и проверке эффективности функционирования элементов и системы зашиты в целом Результаты оформляются в виде предложений (проекта) в кратком сжатом виде, а материалы моделирования - в виде приложения с обоснованием предложений.

В заключение следует отметить, что материалы с предложениями и их обоснованием, в которых раскрываются методы и средства защиты информации, нуждаются в обеспечении высокого уровня безопасности, а обобщенные документы должны иметь наиболее высокий гриф из применяемых в организации.

9. Компьютерные лабораторные работы

Лабораторная работа 1. Исследование методов аналогового скремблирования

Вступление человечества в 21 век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Безопасность связи при передаче речевых сообщений основывается на использовании большого количества различных методов закрытия сообщений, меняющих характеристики речи таким образом, что она становится неразборчивой и неузнаваемой для подслушивающего лица, перехватившего закрытое речевое сообщение. При этом главной целью при разработке систем передачи речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем [1].

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи:

— аналоговое скремблирование;

— цифровое скремблирование (дискретизация речи с последующим шифрованием) [2].

Каждый из этих методов имеет свои достоинства и недостатки, но рассмотрим аналоговое скремблирование

В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется в первую очередь снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры, а их криптостойкость превосходит, и порой довольно значительно, криптостойкость скремблеров. Тем не менее, знать основы функционирования скремблеров, как этап в истории защиты речевой информации, необходимо. Во-первых, аналоговые до сих пор используются там, где невозможно, по ряду причин, использовать другие средства. Во-вторых, фундаментальные принципы и понятия, заложенные в скремблирующие алгоритмы, также распространяются и на другие методы защиты речевых сообщений [2].

Аналоговые скремблеры

Под аналоговым скремблированием понимается изменение характеристик речевого сигнала так, чтобы полученный сигнал, обладая свойствами речевой неразборчивости, занимал такую же полосу частот, что и исходный открытый сигнал. При использовании этого метода в закрытом сигнале присутствуют фрагменты исходного открытого речевого сообщения, преобразованные в частотной или временной областях. Это означает, что злоумышленники могут попытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с цифровыми системами, степень закрытия. Однако новейшие алгоритмы аналогового скремблирования способны обеспечить не только средний, но очень высокий уровень закрытия [1].

Системы скремблирования подразделяются на два класса:

— статические, схема шифрования которых остается неизменной в течение всей передачи сообщения; такие системы не обладают сколько-нибудь значительной стойкостью, но вполне приемлемы как модели реальных систем скремблирования;

— динамические, с дополнительным повышением уровня закрытия информации за счет изменения параметров преобразования сигнала во времени при постоянном генерировании кодовых подстановок в ходе передачи/приема; такие скремблеры принято обозначать термином роллинговые скремблеры.

Аналоговое скремблирование обеспечивает меньшую степень закрытия речевых сигналов по сравнению с цифровыми методами шифрования, однако при практической реализации аналоговые скремблеры более просты, дешевы, применимы в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц и обеспечивают коммерческое качество восстановления речевого сигнала с гарантией достаточно высокой стойкости закрытия речи, передаваемой по каналу связи.

Большинство структур безопасности оснащено профессиональными средствами УКВ радиосвязи зарубежных фирм таких, как Motorola, Kenwood, Icom и др., использующими аналоговые виды модуляции сигнала (частотный или фазовый). Для подобного рода радиосредств в подавляющем большинстве в качестве устройств защиты информации применяются аналоговые речевые скремблеры.

Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временных параметров в различных комбинациях. Скремблированный сигнал может быть передан по каналу связи в той же полосе частот, что и исходный, открытый [1].

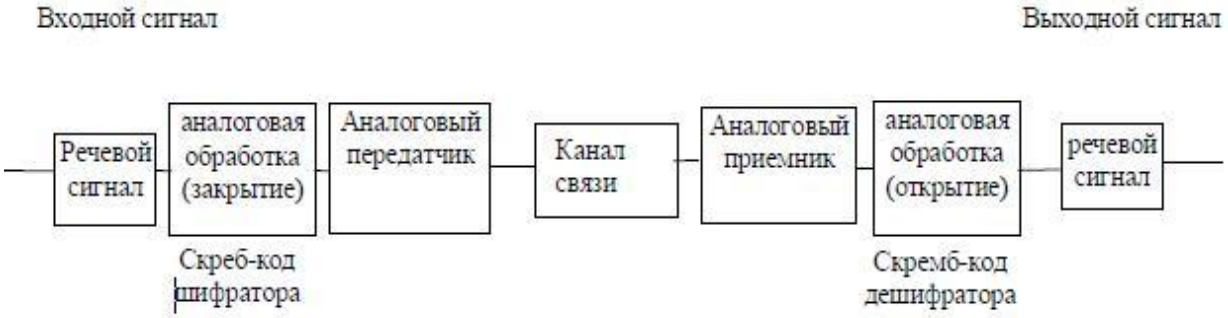


Рис.1 – Обобщенная структурная схема аналогового скремблера

Виды преобразований аналоговых скремблеров

При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Однако в системах подвижной радиосвязи практическое применение нашли в основном частотные и временные методы преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются [1].

При частотных преобразованиях сигнала в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

— частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);

— разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов, их частотные перестановки и частотная инверсия спектра в каждом относительно средней частоты поддиапазона [1].

При временных преобразованиях производится разбиение сигнала на речевые сегменты и применение к ним операций инверсии и перестановок во времени. При этом используются следующие способы закрытия:

— инверсия по времени протяженных сегментов речи;

— временные перестановки коротких фрагментов в сегментах речевого сигнала;

— временные перестановки коротких фрагментов и их инверсия в сегментах речевого сигнала [1].

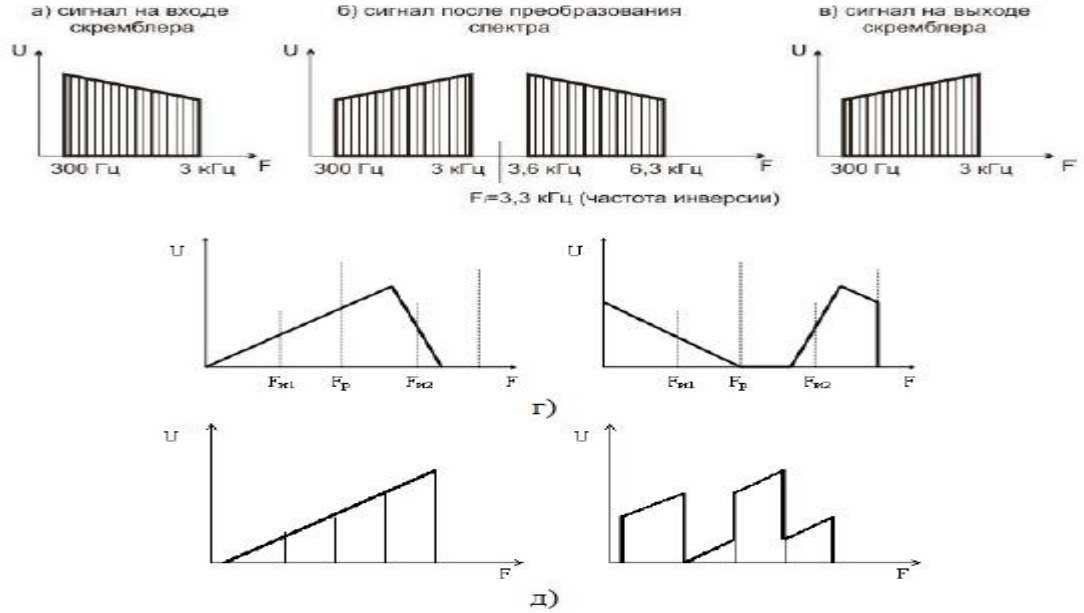
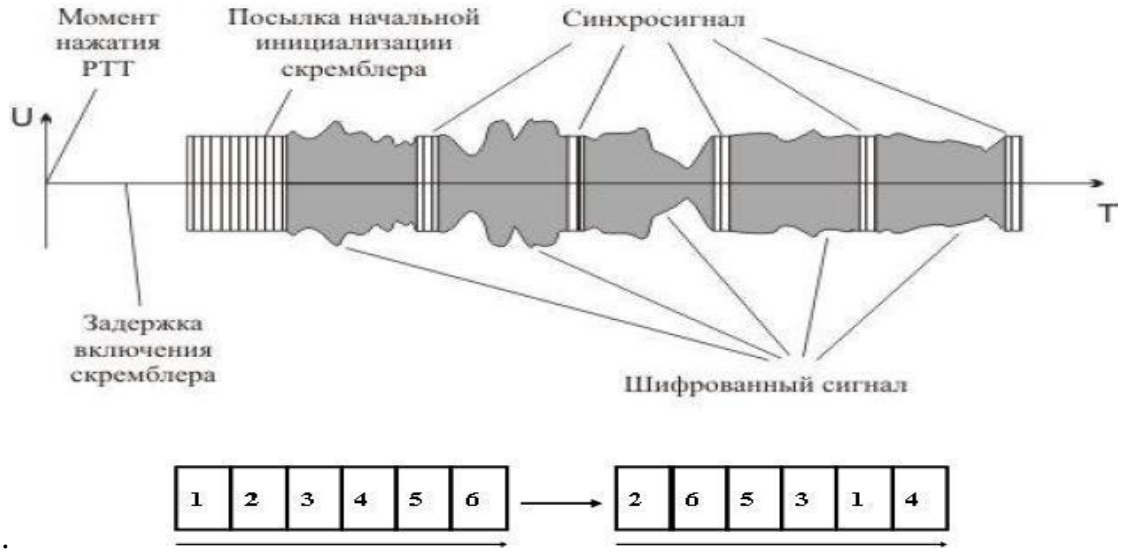


Рис. 2. Инверсия спектра при скремблировании сигнала – а), б), в); последовательность преобразований; – г); частотные перестановки фрагментов спектра сигнала

В скремблерах с временной перестановкой сигнал делится на сегменты и фрагменты (см. рисунок 3.2) над которыми осуществляется перестановка или инверсия, причем сегмент (кадр) может быть, как фиксированным, так и скользящим. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности фрагментов в сегментах, а также создают значительные поддержки при работе, требуют дополнительной синхронизации, поэтому их практическое использование затруднено, но они весьма полезны в системах, где требует простота устройства



.

Рис. 3. Скремблированный сигнал с перестановками во времени фрагментов сегмента речевого сигнала

Комбинированные методы преобразования сигнала предполагают использование одновременно нескольких различных способов скремблирования (как частотных, так и временных), число которых ограничивается, как правило, возможностями технической реализации аналоговых скремблеров [6].

Динамические скремблеры существенно дороже скремблеров с фиксированными параметрами преобразования сигнала, сильнее влияют на характеристики радиосредств и требуют начальной синхронизации. Однако их применение действительно затрудняет возможности перехвата переговоров, в особенности в реальном масштабе времени. Это объясняется тем, что изменение ключевых параметров во времени теоретически делает возможным резкое увеличение количества ключей. Ключом может быть начальное значение генератора псевдослучайной последовательности, в соответствии с которой меняется определенный ключевой параметр [6].

Временные преобразования сигнала в сочетании с изменением ключевых параметров во времени достаточно сложны для реализации и требуют относительно длительной синхронизации, поэтому они пока не нашли свое применение в роллинговых скремблерах. Для способов частотного преобразования сигнала изменяемыми ключевыми параметрами могут быть частота инверсии (для частотного инвертора), частота разбиения полосы сигнала (для полосно-сдвигового инвертора), комбинация частотной перестановки поддиапазонов сигнала (для полосового скремблера). Большинство известных моделей роллинговых скремблеров используют наиболее простой принцип спектрального преобразования – частотный инвертор с изменением частоты инверсии сигнала во времени [2].

Технические характеристики

Основными техническими характеристиками аналоговых скремблеров являются уровень закрытия информации, остаточная разборчивость и качество восстановления сигнала.

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил. В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера [1].

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала. Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров) [1].

Обзор известных моделей скремблеров

Наибольшее количество известных моделей скремблеров реализуют частотную инверсию сигнала. Все они имеют близкие параметры. Одними из первых на отечественном рынке появились модели скремблеров фирмы Selectone (ST-20 и ST-022),

работающие в диапазоне частот 300-2400 Гц и обеспечивающие инверсию сигнала относительно 8 возможных номиналов частот в диапазоне от 2,6 до 3,7 КГц (частота инверсии устанавливается программно).

Простейшие модели скремблеров фирмы Transcrypt SC20-400 и SC20-401 обладают характеристиками, аналогичными ST-20 и ST-022; речевой диапазон частот, 4 варианта частоты инверсии [1].

Сравнительная характеристика скремблеров по основным параметрам приведена в таблице 4.1.

Более сложное преобразование сигнала предлагают полосно-сдвиговые инверторы, разработанные НТЦ "ИНТЕР-ВОК" Принцип работы микросборок 04ХК011 ("Сонет"), 04ХК012, 04ХК014А, 04ХК015А, 04ХК017А состоит в разделении речевого спектра на две части, низкочастотную и высокочастотную, каждая из которых разворачивается вокруг своих средних частот. Все они работают в диапазоне речевых частот - 300-3400 Гц. Указанные скремблеры обладают повышенной по сравнению с частотными инверторами степенью закрытия информации. В технических данных указывается, что скремблеры обеспечивают остаточную разборчивость речи не более 10 %. В то же время гарантируется сохранение высокого качества речи при прослушивании с помощью радиостанции, оснащенной аналогичным скремблером (сохранение 1 класса разборчивости при измерении по методике ГОСТ 16600-72) [1].

Известны скремблеры для эффективной защиты телефонных переговоров в сетях, работающих по GSM стандарту. Специально разработанный скремблер GUARD GSM, будучи эконом-вариантом, отлично маскирует речь, передаваемую по каналам GSM связи. Данное устройство соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры [1].

Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановки звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс дуплексный. Начало разговора, как правило, начинается в открытом режиме и далее по обоюдной команде устройства, переключаются в режим скремблирования [1].

Программная реализация виртуальной модели скремблера

Программную реализацию виртуальной модели скремблера можно выполнить в среде LabVIEW, Simulink или на одном из языков объектно-ориентированного программирования. Приведенная реализация программной модели выполнена в виде виртуальных приборов, созданных в среде LabVIEW. Данная программная система моделирует скремблер работающий с телефонным каналом связи на частоте от 200 Гц до 3,4 КГц. В модели представлены несколько видов операций скремблирования [1]:

— временной статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки;

— временной скремблер с инверсией;

— полосовой частотный статический скремблер, производящий операции

— над блоками фиксированного размера с фиксированным порядком перестановки, использует фильтрацию, инверсию спектра, преобразование частоты;

— полосовой частотный статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки, использует прямое и обратное БПФ;

— инвертирующий частотный скремблер, производящий операции над блоками фиксированного размера, использующий прямое и обратное БПФ, инверсия идет относительно средней точки спектральной последовательности.

В качестве исходных сигналов скремблера использованы звуковые файлы в формате WAV, записанные с частотой дискретизации 8 КГц в формате моно. Скремблер может выполнять загрузку звуковых файлов в формате WAV, их скремблирование или

дескремблирование по одному из нескольких алгоритмов с изменяемыми параметрами, запись результата в файлы в формате WAV, а также визуализировать и озвучить как исходный, так и обработанный звук [1].

Временное скремблирование

Разработан виртуальный прибор для осуществления временных видов скремблирования/дескремблирования, лицевая панель которого для осуществления скремблирования речевого сигнала во временной области на основе его инверсии приведена на рис.5, а фрагмент диаграммной панели – на рис .6. На лицевую панель прибора выведены: временные диаграммы входного сигнала, скремблированного сигнала, все необходимые регулировочные ручки для настроек параметров скремблера и органы индикации параметров речевого сигнала.

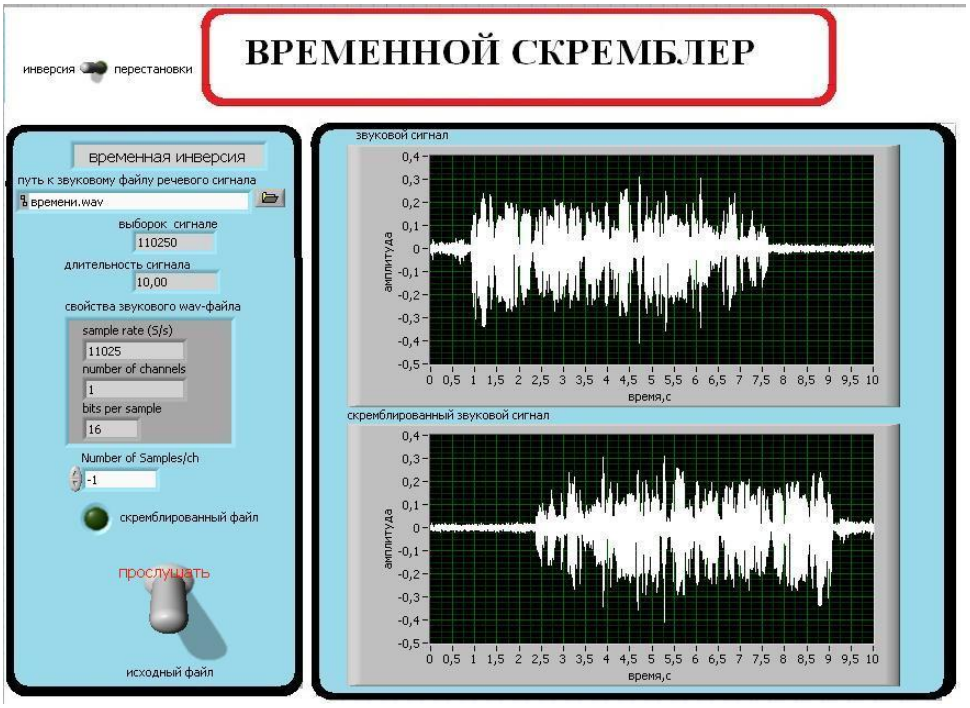


Рис. 4 – Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала на основе временной инверсии

Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска и для записи скремблированного сигнала в файл, а также блоки для преобразований типов данных для осуществления временной инверсии. Лицевая панель виртуального прибора при переключении тумблера для осуществления скремблирования речевого сигнала во временной области на основе перестановок временных сегментов сигнала приведена на рис.3, а фрагмент диаграммной панели – на рис.4. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, осуществления временных перестановок с фиксированным ключом и для записи скремблированного сигнала в файл. Временные перестановки на приведенном виртуальном приборе на рисунке 3 выбраны с фиксированным ключом: 87214365, где цифры обозначаю номер временного фрагмента в сегменте исходного речевого сигнала [1].

При программировании алгоритма на диаграммной панели можно использовать case-структуру для выбора временной инверсии и временных перестановок. Дальнейшая модернизация скремблера предусматривает задание ключей скремблирования при перестановке временных сегментов с помощью case-структуры. Это же касается и модели дескремблера.

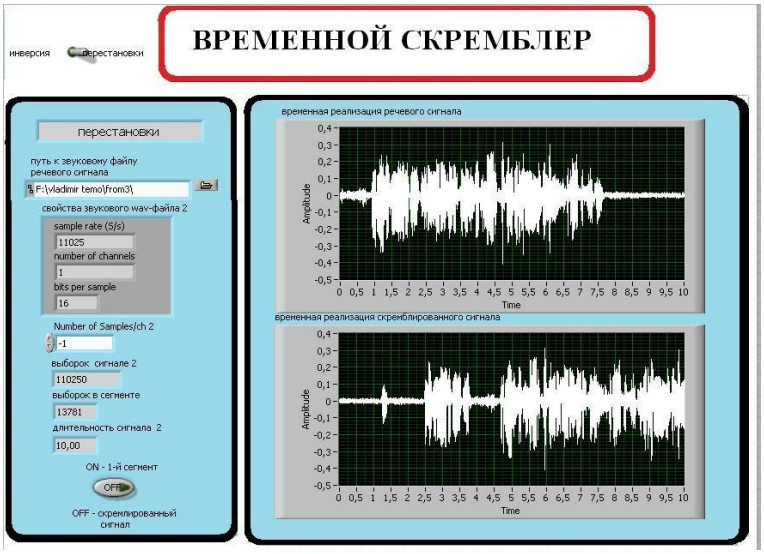


Рис. 5 – Лицевая панель виртуального прибора для осуществления временного скремблирования речевого сигнала с перестановками

Виртуальный прибор позволяет при каскадном наращивании разработанных библиотечных модулей временного скремблирования/ дескремблирования реализовать код скремблирования любой сложности.

— Необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала.

— Основным источником шума при скремблировании и дескремблировании является длительность элементарного временного сегмента при разбиении, которая в пределе равна шагу дискретизации сигнала.

— При учете всех выше сказанных особенностях и должных настроек элементов виртуального прибора, обеспечивается хорошее закрытие информации, а затем её восстановление при дескремблировании с хорошей словесной разборчивостью [1].

Частотное скремблирование

Реализовать виртуальные приборы для осуществления частотного полосового скремблирования можно различными способами: параллельно-последовательной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с использованием БПФ и др. Приведем некоторые варианты реализации первых двух способов.

Параллельно-последовательная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на две полосы, осуществление их перестановок и инверсии спектра, а затем последовательно к каждому частотному диапазону применения аналогичных преобразований. Таким образом, можно последовательно увеличивать число частотных полос при разбиении спектра в 2 раза (2 полосы, 4, 8, 16, и т.д.), тем самым, увеличивая количество ключей скремблирования. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 4 полосы) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования [1].

Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена на рисунке 7.7, а диаграммная панель – на рисунке 7.8.

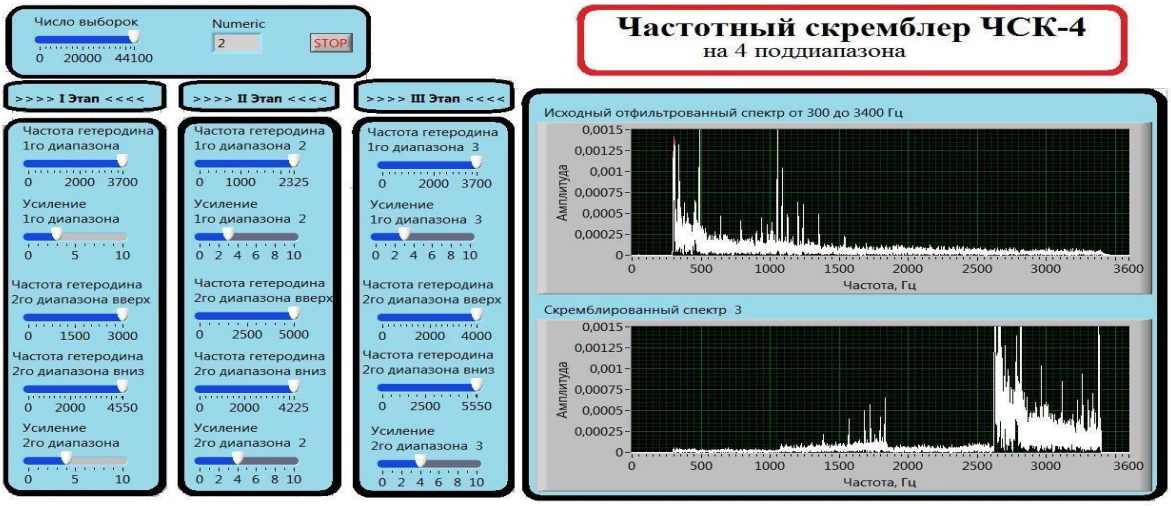


Рис. 6. Лицевая панель виртуального прибора частотного скремблирования речевого сигнала

На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл. Скремблер состоит из трёх последовательно соединенных смесителей с подключенными регулировочными ручками.

В качестве фильтра выбран эллиптический фильтр 6-го порядка из-за высокой крутизны АЧХ, сопровождающейся колебательным характером плоской вершины в полосе пропускания, и наличием боковых лепестков в полосе заграждения.

Каждый смеситель (см. рисунок 7.9) делит входной сигнал на два диапазона частот. На 1 этапе сигнал делится по 1550Гц. Первый диапазон (300Гц-1850Гц) инвертируется и перемещается (1850Гц-3400Гц) с помощью гетеродина с частотой 3700Гц (см. рисунок 7.10) [1].

Второй диапазон (1850Гц- 3400Гц) перемещается (300Гц-1850Гц) без инвертирования, с помощью двух гетеродинов с частотами 3000Гц и 4550Гц.

На выходе 1-го смесителя два диапазона складываются. В результате получается скремблированный сигнал I этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход второго смесителя, где делится на два диапазона. Первый диапазон (2625Гц-3400Гц) перемещается (300Гц-1075Гц) без инверсии, с помощью гетеродина с частотой 2325Гц.

Второй диапазон (300 Гц-2625Гц) перемещается (1075 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 5000Гц и 4225Гц.

На выходе 2-го смесителя два диапазона складываются. В результате получается скремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего смесителя, где делится на два диапазона. Первый диапазон (300Гц-1850Гц) перемещается (1850Гц-3400Гц) с инверсией, с помощью гетеродина с частотой 3700Гц.

Второй диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850Гц) без инверсии, с помощью двух гетеродинов с частотами 4000Гц и 5550Гц [1].

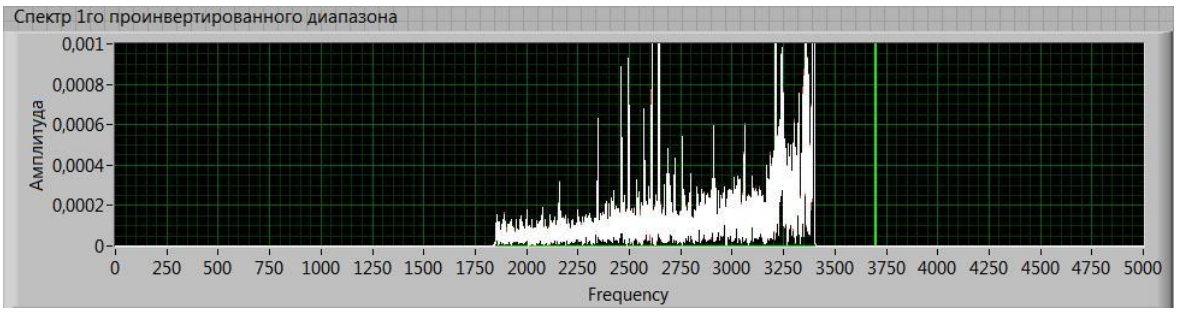


Рис. 7. Спектр первого проинвертированного диапазона

На выходе 3-го смесителя два диапазона складываются. В результате получается скремблированный сигнал III этапа на частотах от 300Гц до 3400Гц – спектр результирующего скремблированного сигнала (см. рисунок 6.11).

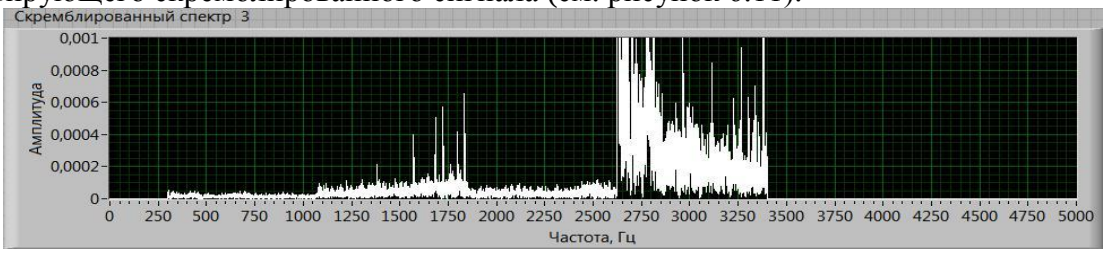


Рис. 8. Спектр скремблированного сигнала третьего этапа

Дескремблер. Для восстановления скремблированного речевого сигнала был спроектирован частотный дескремблер. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр дескремблированного

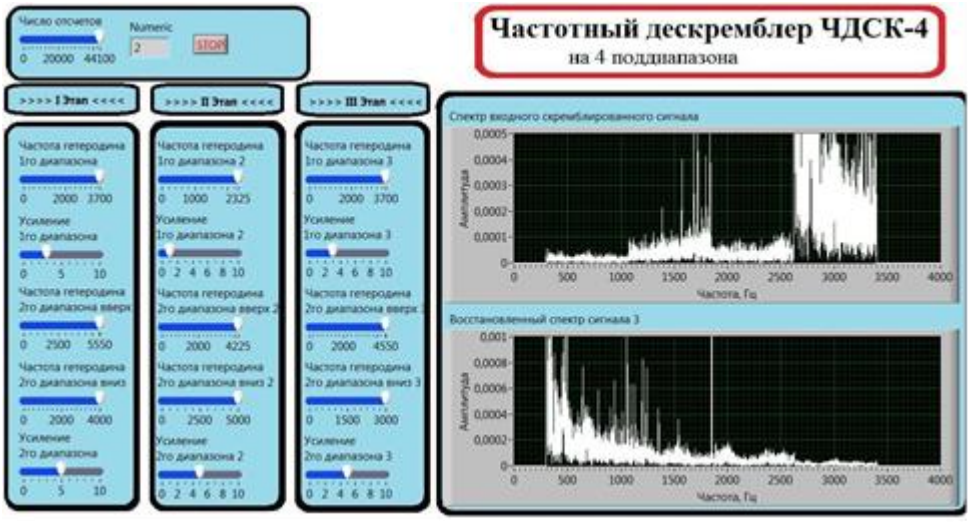


Рис. 9. Лицевая панель виртуального прибора дескремблера: три последовательно соединенных разделителя с регулировочными ручками

Каждый разделитель делит входной сигнал на два диапазона частот (см. рисунок 6.13). Сигнал поступает на вход первого разделителя, где первый диапазон (1850 Гц- 3400 Гц) инвертируется и перемещается (300 Гц-1850 Гц) с помощью гетеродина с частотой 3700Гц.

Второй диапазон (300 Гц-1850 Гц) перемещается (1850Гц-3400Гц) без инвертирования при помощи двух гетеродинов с частотами 5550 Гц и 4000 Гц

На выходе 1-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал I этапа на частотах от 300Гц до 3400 Гц.

Далее сигнал поступает на вход второго разделителя, где делится на два диапазона. Первый диапазон (300Гц-1075Гц) перемещается (2625Гц-3400Гц) без инверсии, при помощи гетеродина с частотой 2325Гц.

Второй диапазон (1075Гц-3400Гц) перемещается (300 Гц-2625Гц) без инверсии, с помощью двух гетеродинов с частотами 4225 Гц и 5000 Гц [1].

На выходе 2-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего разделителя, где делится на два диапазона. Первый диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850 Гц) с инверсией, с помощью гетеродина с частотой 3700 Гц.

Второй диапазон (300 Гц-1850Гц) перемещается (1850 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 4550Гц и 3000Гц.

На выходе 3-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал III этапа на частотах от 300Гц до 3400Гц.

Виртуальные приборы, осуществляющие аналоговое частотное скремблирование речевых сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Параллельная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на заданное число полос, осуществление их перестановок и инверсии спектра. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 8 полос) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования [1].

Исходный спектр речевого сообщения разбивается на 8-поддиапазонов, как изображено на рисунок

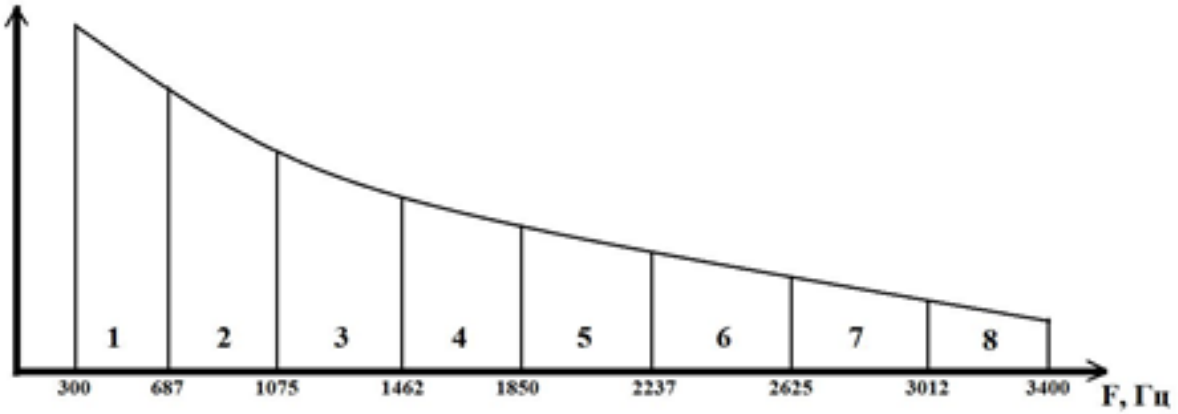


Рис. 9. Разбиение сигнала на 8 поддиапазонов

В зависимости от кода скремблера, диапазоны инвертируются и расставляются в определенном порядке, например, как показано на рисунке 6.16

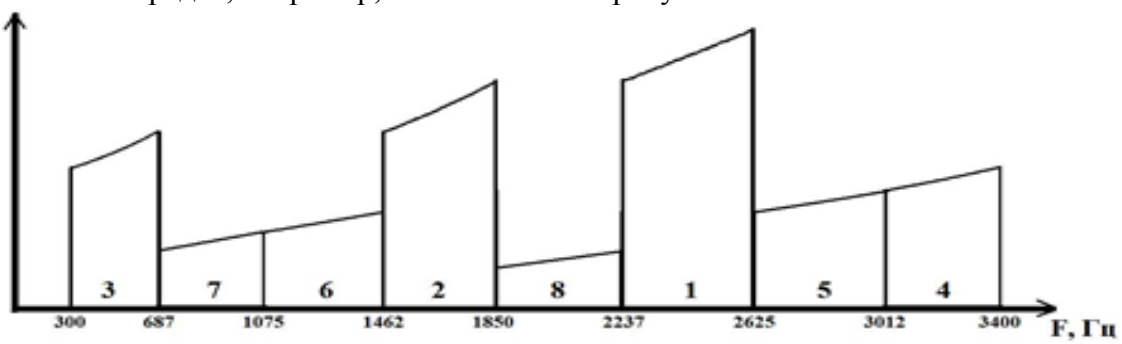


Рис. 10. Структура спектра после скремблирования

Диаграммная панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена

на рисунке 7.17. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера [1]. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл

Исходный сигнал подается на 8 полосовых эллиптических фильтров 7-го порядка, после чего, для того, чтобы проинвертировать спектр и перенести его в диапазон 2237 Гц – 2625 Гц, используется гетеродинное преобразование частоты с частотой генератора 2925 Гц, в результате. Теперь, чтобы отделить необходимую часть спектра, сигнал пропускается через полосовой эллиптический фильтр 6-го порядка. Параметры 2-го фильтра выбираются с меньшим порядком и большим частотным захватом фильтруемого спектра, чтобы меньше искажать форму сигнала [1].

Элемент (SubVI) является вложенным виртуальным прибором, который выполняет фильтрацию и перестановку поддиапазонов, формируя на выходе два канала. После усиления они объединяются в один канал, и сигнал записывается в файл. Диаграммная панель вложенного виртуального прибора представлена на рисунке

На выходе вторых фильтров используются сумматоры для объединения 1, 2, 4 и 7-го поддиапазонов во второй канал и объединения 3, 5, 6 и 8-го поддиапазонов в первый канал.

На рисунке представлена лицевая панель виртуального прибора скремблера, на котором видно, что поддиапазоны в скремблированном сигнале не взаимодействуют

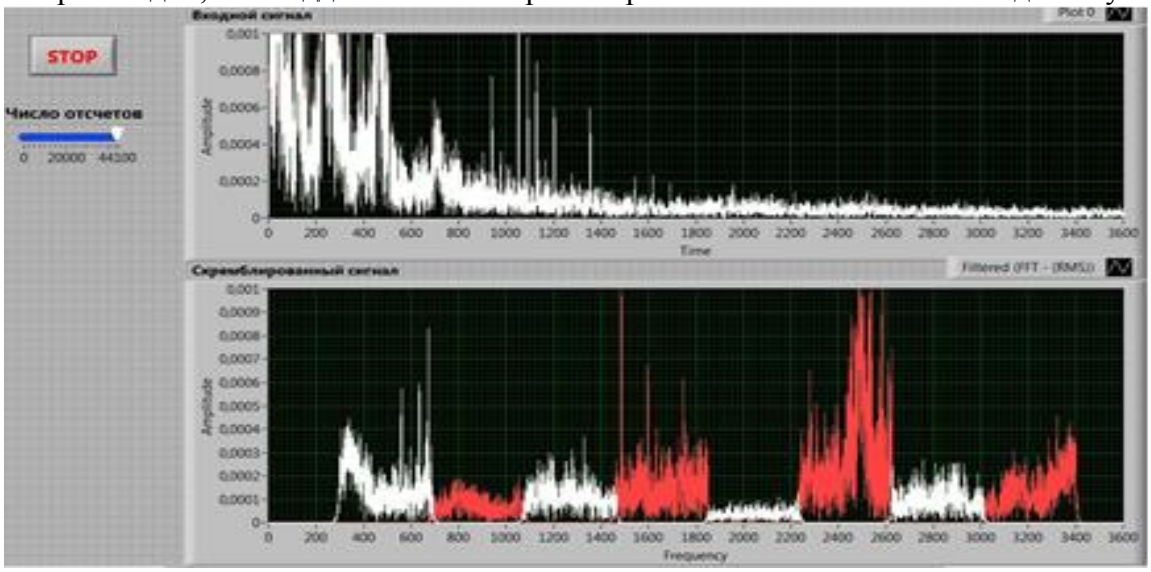


Рис. 11. Лицевая панель виртуального прибора скремблера

Анализ качества и криптостойкости скремблеров

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил.

В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера.

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала [1].

Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров). В связи с вышесказанным, лучше всего речь закрывает мозаичный скремблер с шестнадцатью возможными положениями ключа и инверсией, и перестановками по времени, на втором месте по защищенности – шестнадцати диапазонный скремблер также с шестнадцатью возможными положениями ключа, но с отсутствием скремблирования по времени. Замыкает тройку частотный четырех диапазонный скремблер. Временные скремблеры, в данном определении уровня закрытия речевой информации, расположились на последнем месте, по той причине, что они статичны и у них отсутствует возможность изменения ключей. Справедливости ради стоит отметить, что на слух, временной скремблер более лучше закрывает информацию, чем скажем четырех диапазонный частотный скремблер. Оценка разборчивость речи мной согласно ГОСТу Р 50840–95 затруднительна, так как требует специальных знаний, средств и обученных людей [1].

Был разработан программный комплекс, позволяющий проводить аналоговое скремблирование. Таким образом, из описанных моделей скремблеров/дескремблеров следуют следующие выводы:

— даже при разделении сигнала на четыре поддиапазона, скремблированный сигнал имеет низкую словесную разборчивость, что указывает на сильное закрытие информации виртуальным прибором;

— так как в данном устройстве используются гетеродины, к ним должны предъявляться жесткие требования, иначе вследствие нестабильности их частоты полезный сигнал будет подавлен фильтром, что снизит качество восстанавливаемого сигнала;

— в результате гетеродинного преобразования полезный сигнал теряет часть энергии, в виду этого необходимо производить усиление в каждом диапазоне на всех этапах скремблирования и дескремблирования;

— необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала;

— Основным источником шума при скремблировании и дескремблировании являются эллиптические фильтры

— Также при проектировании прибора необходимо учитывать, что фильтр с высоким порядком является высокодобротной системой и имеет долгий незатухающий отклик - «звон», что влечет за собой появление помехи

Виртуальные приборы, осуществляющие аналоговое временное, частотное скремблирование речевых сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного, временного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Исследование аналогового временного скремблера

Временные скремблеры основаны на двух основных способах закрытия: инверсии по времени сегментов речи и их временной перестановке. В скремблерах с временной

инверсией речевой сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени - с конца. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности сегментов. Для достижения неразборчивости медленной речи необходимо, чтобы длина сегмента составляла около 250 мс. Это означает, что задержка системы будет равна примерно 500 мс, что может оказаться неприемлемым для некоторых приложений.

Для повышения уровня закрытия прибегают к способу перестановки временных отрезков речевого сигнала в пределах фиксированного кадра (рисунок 1). Правило перестановок является ключом системы, изменением которого можно существенно повысить степень закрытия речи. Остаточная разборчивость зависит от длительностей отрезков сигнала и кадра и с увеличением последнего уменьшается.

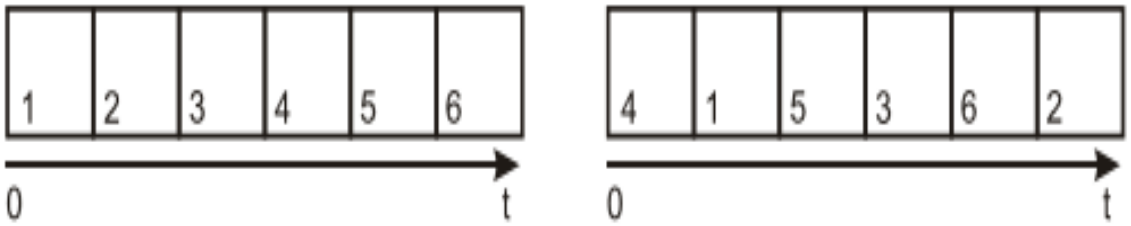


Рис. 12. Схема работы временного скремблера с перестановкам
и в фиксированном кадре

Главным недостатком скремблера с фиксированным кадром является большая величина времени задержки системы, равная удвоенной длительности кадра. Этот недостаток устраняется в скремблере с перестановкой временных отрезков речевого сигнала со скользящим окном. В нем число комбинаций возможных перестановок ограничено таким образом, что задержка любого отрезка не превосходит установленного максимального значения. Каждый отрезок исходного речевого сигнала как бы имеет временное окно, внутри которого он может занимать произвольное место при скремблировании. Это окно скользит во времени по мере поступления в него каждого нового отрезка сигнала. Задержка при этом снижается до длительности окна.

Ход работы

Для проведения лабораторной работы понадобится звуковой файл в формате wav, для его создания необходимо открыть программу Audacity, рисунок

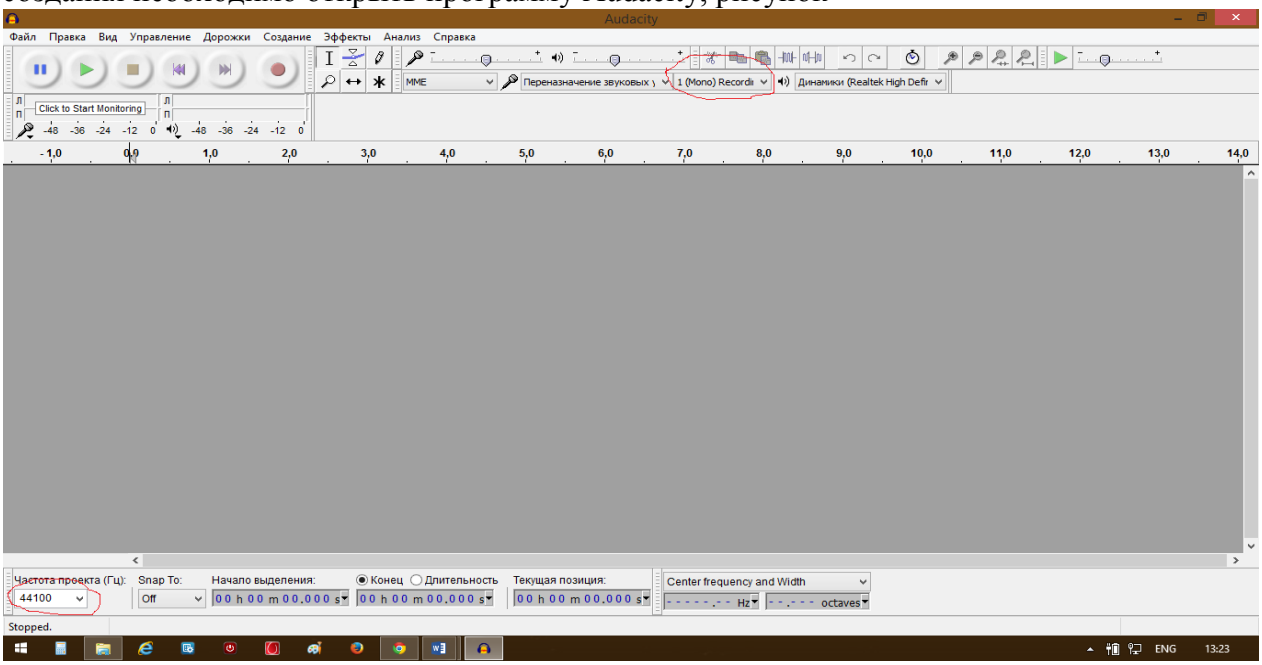


Рис. 13. Окно программы Audacity с нужными настройками (выделено красным).

После этого нужно нажать кнопку запись (круглая кнопка с красным кругом в центре), и записать.

Затем нужно нажать на копку стоп. В меню нажать Файл->Export Audio, в появившемся окне нужно выбрать место куда следует сохранить файл, задать имя файла и убедиться что в поле тип файла выбрано значение: WAV (Microsoft) signed 16-bit PCM.

Для начала работы нужно запустить файл test.vi, запустить программу, установить количество сэмплов, и нажать кнопку старт, в появившемся окне следует выбрать файл, который был записан с помощью программы Audacity.

После этого сигналы исходного и скремблированного файла отображатся на соответствующих экранах, после этого появится окно для выбора места сохранения скремблированного файла.

Инверсный скремблер

Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

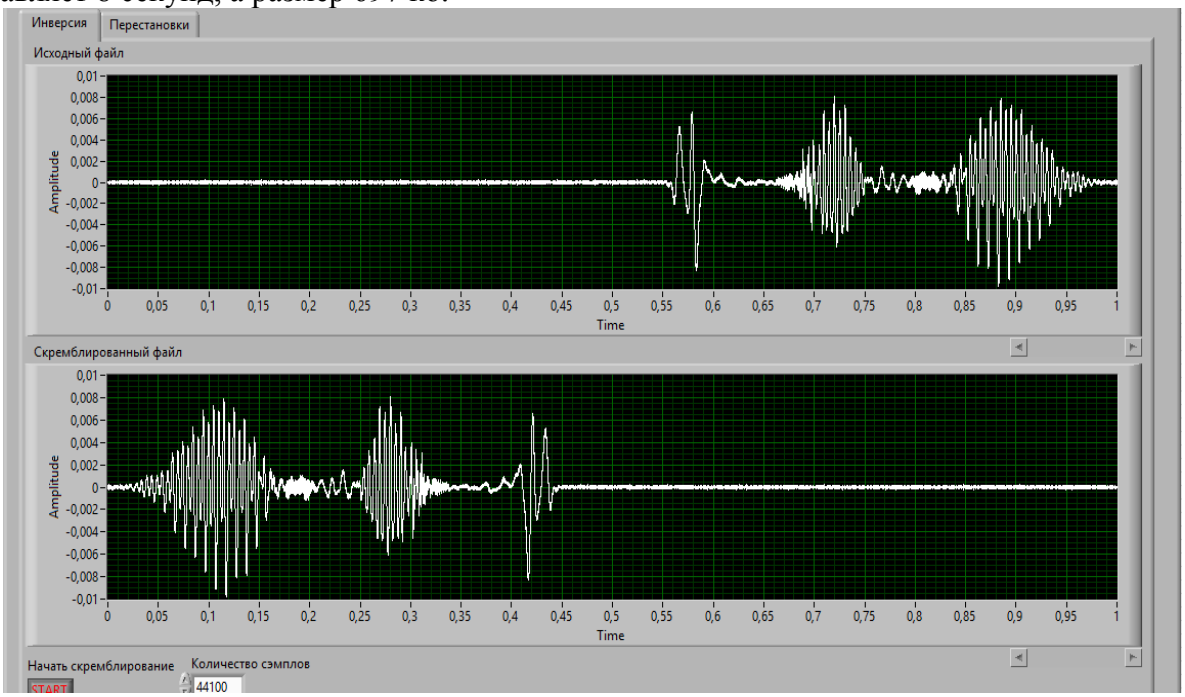


Рис. 14. Результат работы инверсного скремблера с количеством семплов 44100.

Параметры выходного файла: длительность 1 секунда, размер файла 86,1 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного

файла.

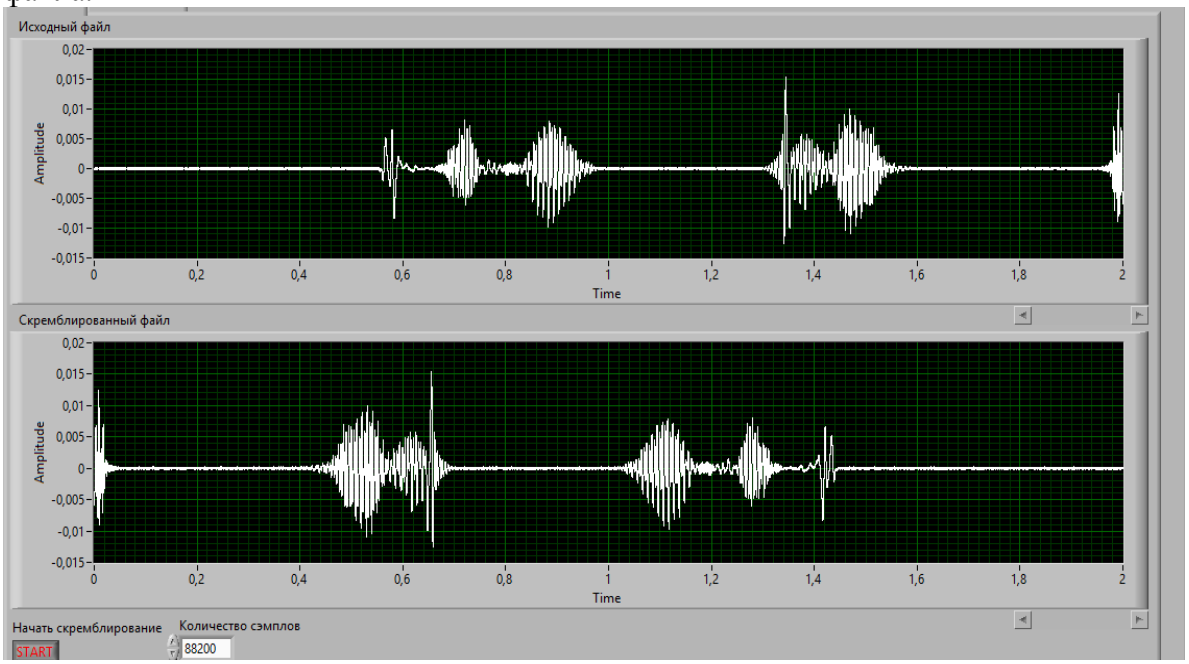


Рис. 15. Результат работы инверсного скремблера с количеством семплов 88200.

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла

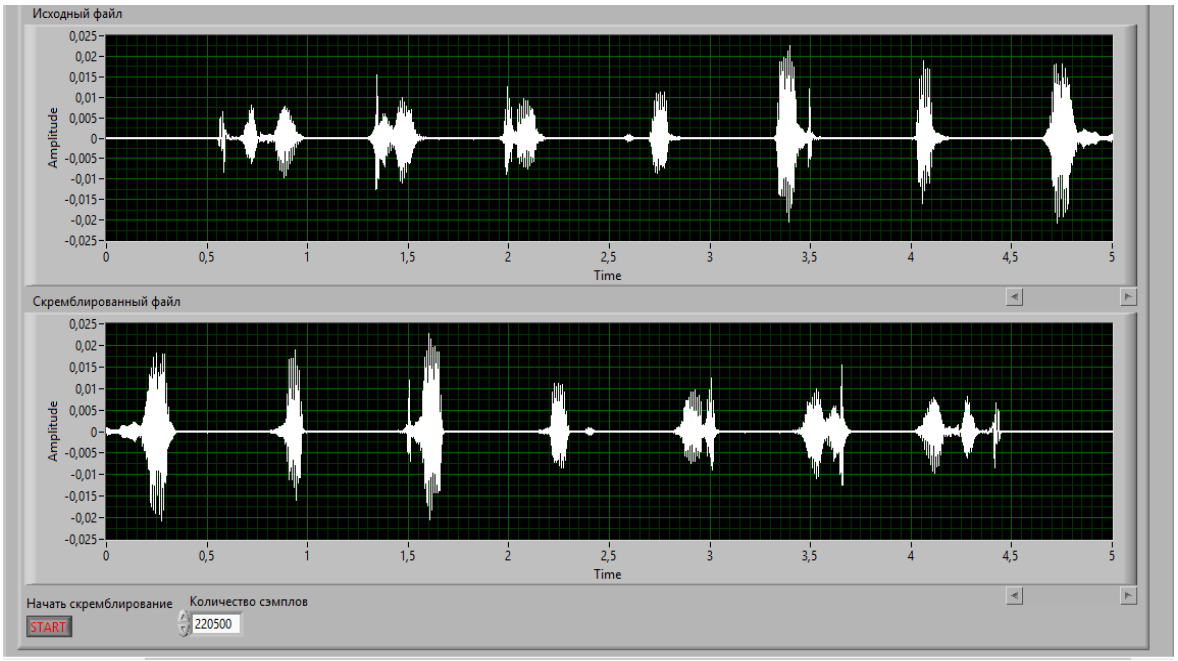


Рис. 16. Результат работы инверсного скремблера с количеством семплов 220500.

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

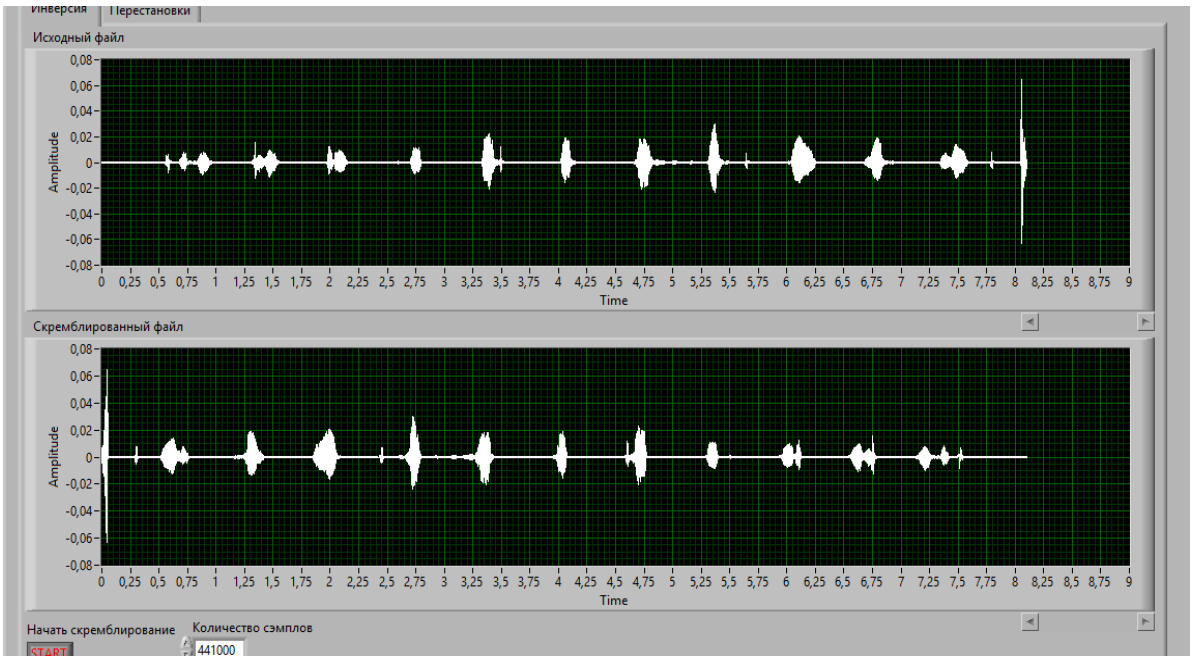


Рис. 17. Результат работы инверсного скремблера с количеством семплов 441000.

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

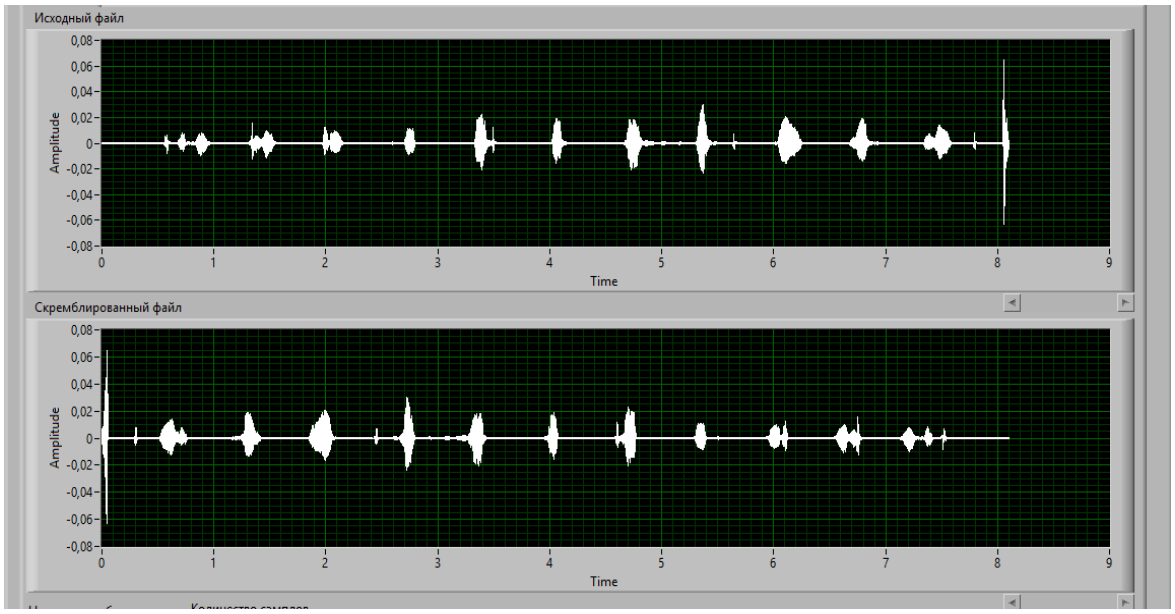


Рис. 18. Результат работы инверсного скремблера с количеством семплов 661500.

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

Скремблер перестановки

Задавая количество семплов 44100*n где n=1,2,5,10,15 посмотрим, как изменится выходной файл.

Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

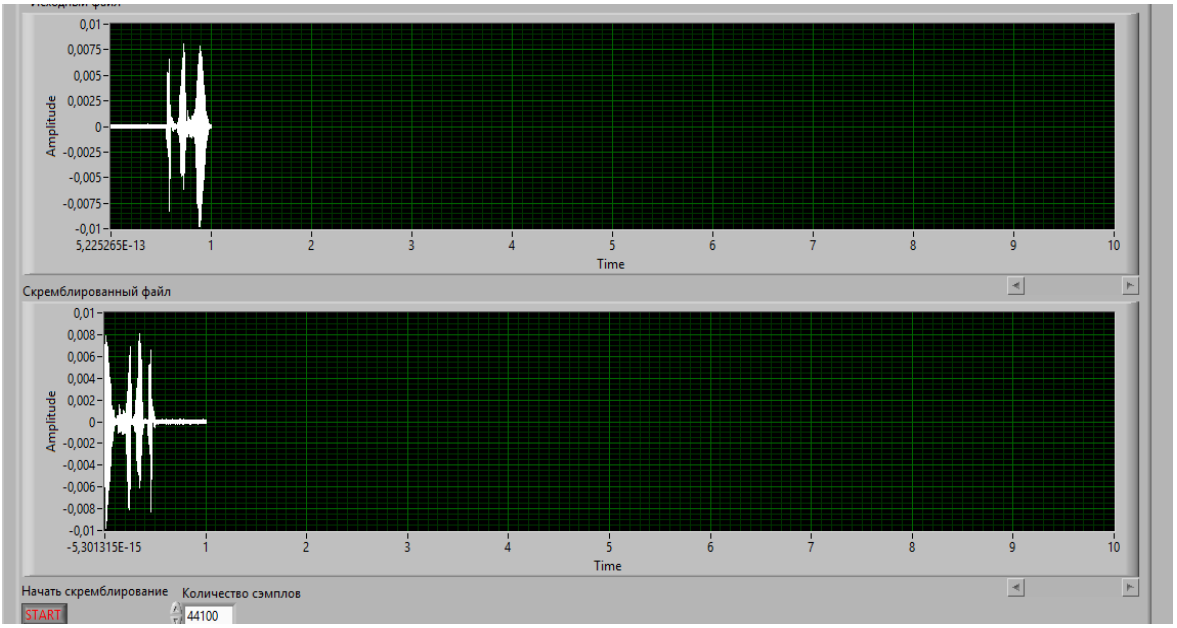


Рис. 19. Результат работы скремблера перестановки с количеством семплов 44100.

Параметры выходного файла: длительность 1 секунда, размер файла 81,1 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного файла.

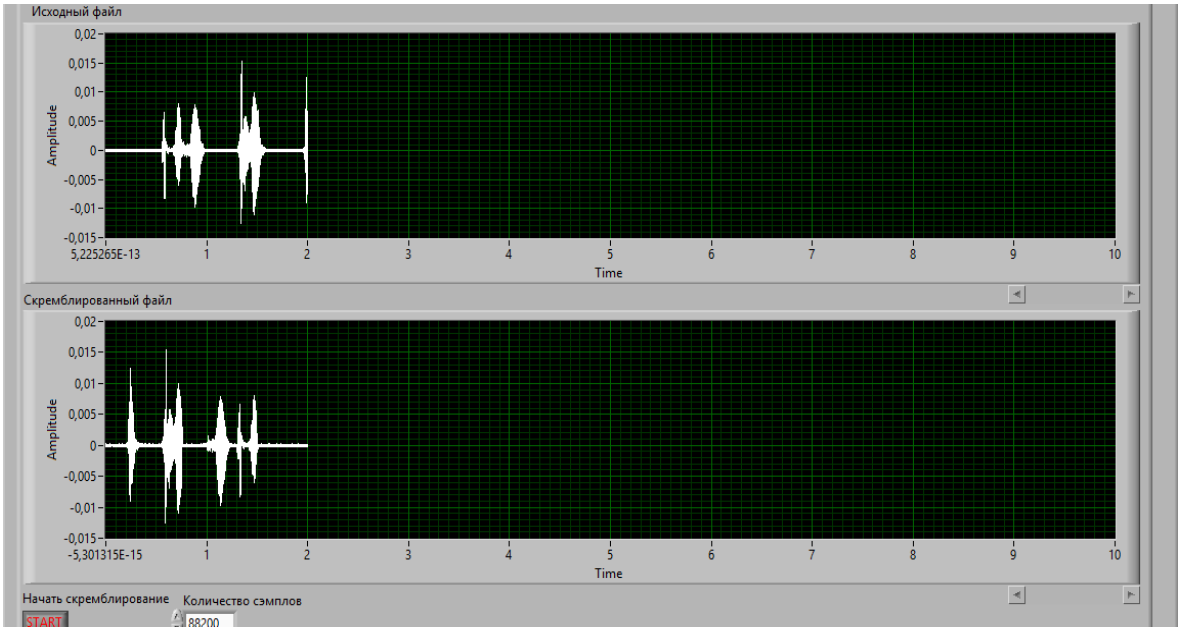


Рис. 20. Результат работы скремблера перестановки с количеством семплов 88200.

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла.

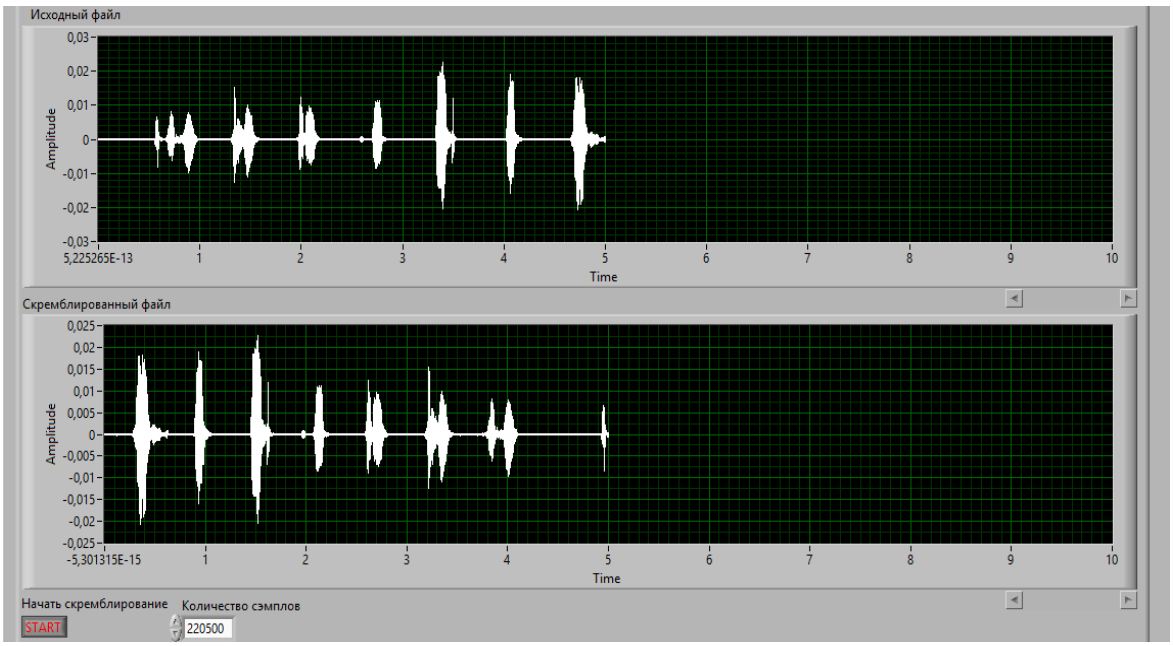


Рис. 21. Результат работы скремблера перестановки с количеством семплов 220500.

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб.

Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

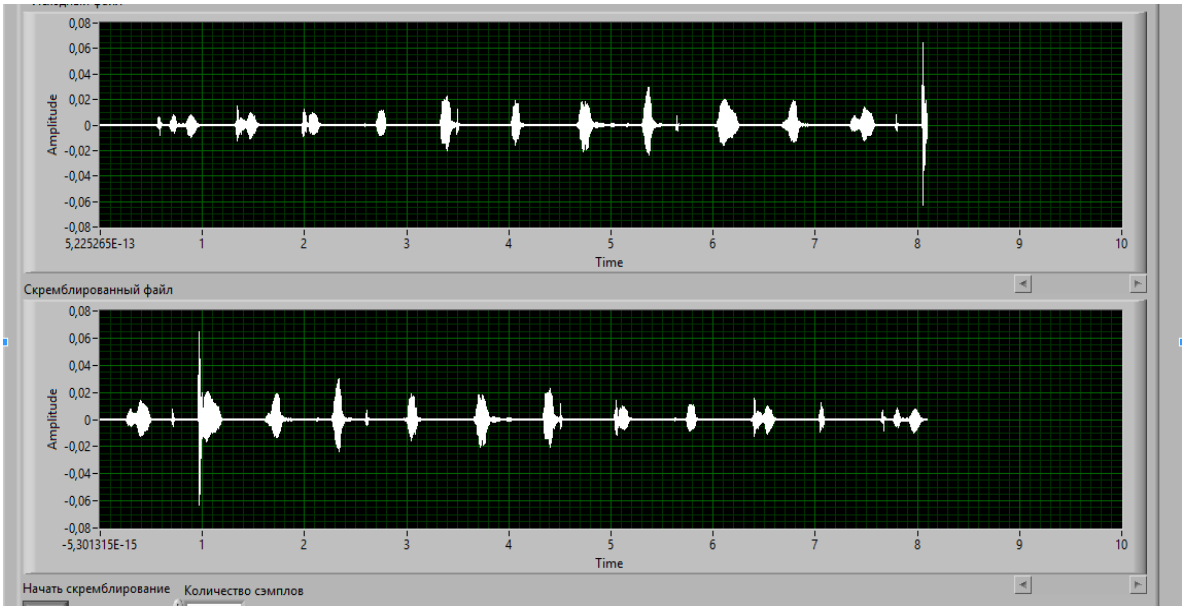


Рис. 22. Результат работы скремблера перестановки с количеством семплов 441000.

Параметры выходного файла: длительность 8 секунд, размер файла 497 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

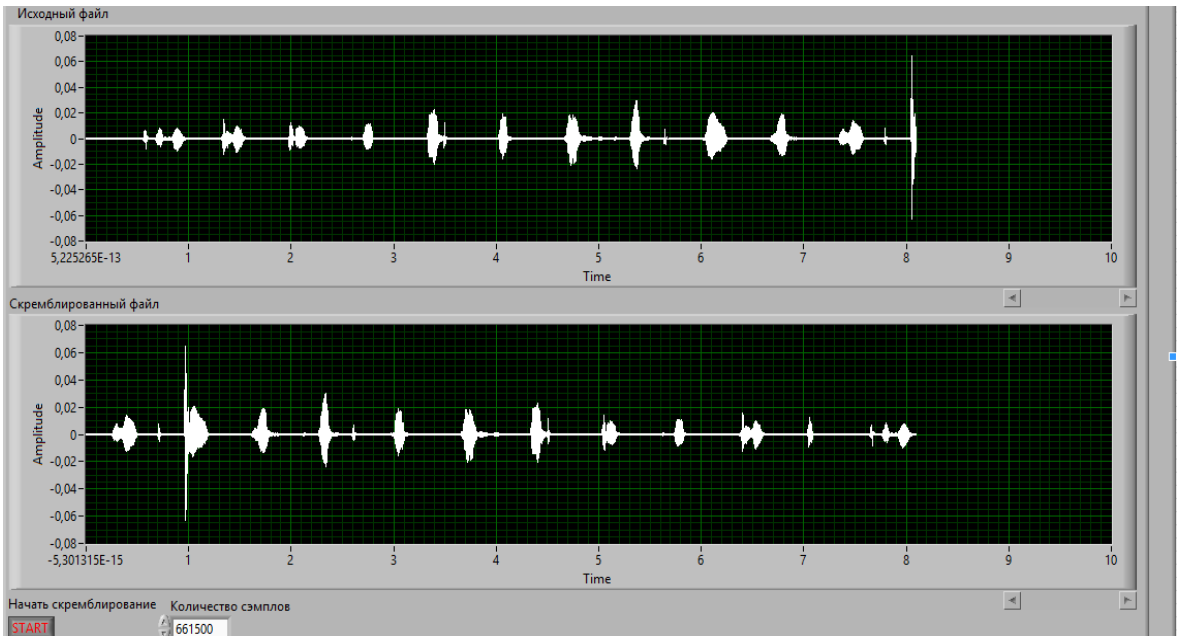


Рис. 23. Результат работы скремблера перестановки с количеством семплов 661500. Параметры выходного файла: длительность 8 секунд, размер файла 497 кб.

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

Лабораторная работа. 2. Скремблирования аудиосигнала с использованием Вейвлет преобразования

Запись аудио сигнала

Для записи аудиосигнала использовались встроенные средства программы MatLab. Изначально для записи голосового сообщения необходимо знать состояние системы и ID подключенных устройств.

Воспользовавшись следующим программным кодом:

```
devinfo = audiodevinfo;

disp('Input devices');
for i = 1 : size(devinfo.input, 2) devinfo.input(i)
end

disp('Output devices');
for i = 1 : size(devinfo.output, 2) devinfo.output(i)
end
```

Получаем сведения о системе представленные на рисунке 1.

```
ans =

          Name: 'Первичный звуковой драйвер (Windows DirectSound)'
    DriverVersion: 'Windows DirectSound'
            ID: 2


ans =

          Name: 'Динамики (Realtek High Definition Audio) (Windows DirectSound)'
    DriverVersion: 'Windows DirectSound'
            ID: 3


ans =

          Name: 'Realtek Digital Output (Realtek High Definition Audio) (Win...'
    DriverVersion: 'Windows DirectSound'
            ID: 4


ans =

          Name: '1 - LG IPS FULLHD (AMD High Definition Audio Device) (Windo...'
    DriverVersion: 'Windows DirectSound'
            ID: 5


ans =

          Name: 'Realtek Digital Output(Optical) (Realtek High Definition Au...'
    DriverVersion: 'Windows DirectSound'
            ID: 6
```

Рис.1. Сведения о системе

Далее зная параметры системы возможно произвести запись аудиосигнала с помощью встроенных в MatLab функций. Для этого был написан следующий программный код:

```
Fs = 8000; % Количество отсчетов nBits = 16; % Битов на отсчет nChannels = 2; % Количество каналов
deviceID = 1; % ID микрофона подключенного к компьютьеру recObj = audiorecorder(Fs, nBits, nChannels, deviceID); get(recObj)

nSeconds = 10;

% Запись голоса и графическое представление записанного сигнала
% Запись в течении nSeconds секудн disp('Start speaking.') recordblocking(recObj, nSeconds); disp('End of Recording.');

% Проигрышь записанного голосового собщения. play(recObj);

% Получение  аудиоданных myRecording = getaudiodata(recObj);

% Графическое представление plot(myRecording);
%Сохранение каналов x1=myRecording(:,1); x2=myRecording(:,2); save Record1;
save Chanel1 x1; save Chanel2 x2;
```

В результате выполнения программы на экран будет выведен график отображающий записанные аудиоданные.

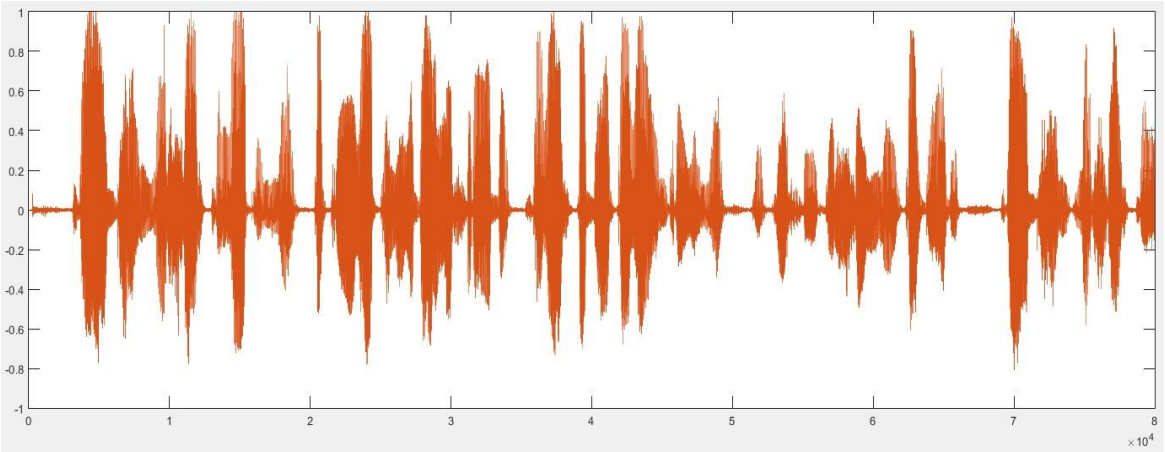


Рис.2. Записанные аудиоданные

Быстрое вейвлет преобразование сигнала

Благодаря своим частотно-временным свойствам вейвлет- преобразование предоставляет широкий спектр возможностей для работы с различного рода сигналами. Помимо классического применения в виде фильтрации и сжатия, вейвлет преобразования являются удобным аппаратом для работы с сигналами в области информационной безопасности. Например, вейвлет преобразование достаточно часто упоминается в различных разделах стеганографии. Так же на основе БВП возможно выполнить сокрытие аудио информации одновременно во временной и частотной области.

Для выполнения быстрого вейвлет-преобразования был разработан следующий код:

```
%Загружаем файл с одним из каналов load('Chanel1.mat');
%имя вейвлета wname='sym4'; lev=4; x=x1';
[dec,struct]=wavedec(x1,lev,wname);
% Вектор dec содержит столбец данных состоящий последовательно приписанных
% уровенй разложения, struct содержит информацию о кол-ве элементов в
% разложении для выделения определенного разложения из dec
% Извлечение коэффициентов разложения sa4 = appcoef (dec, struct, wname,4); sd4= detcoef (dec, struct, 4);
sd3= detcoef (dec, struct, 3); sd2= detcoef (dec, struct, 2); sd1= detcoef (dec, struct, 1);
% Графическая поддержка subplot (711)
plot (x1), title ('Исходный сигнал') subplot (712)
plot (sd1), ylabel ('sd1') subplot (713)
plot (sd2), ylabel ('sd2') subplot (714)
plot (sd3), ylabel ('sd3') subplot (715)
plot (sd4), ylabel ('sd4') subplot (716)
plot (sa4), ylabel ('sa3')
x2 = waverec (dec, struct, wname);
% Рисуем восстановленный сигнал subplot (717);
plot (x2), title ('Восстановленый сигнал'); save wav_dec;
```

На рисунке 3. изображено разложение и восстановление аудиосигнала при помощи БВП с использованием симлета 4.

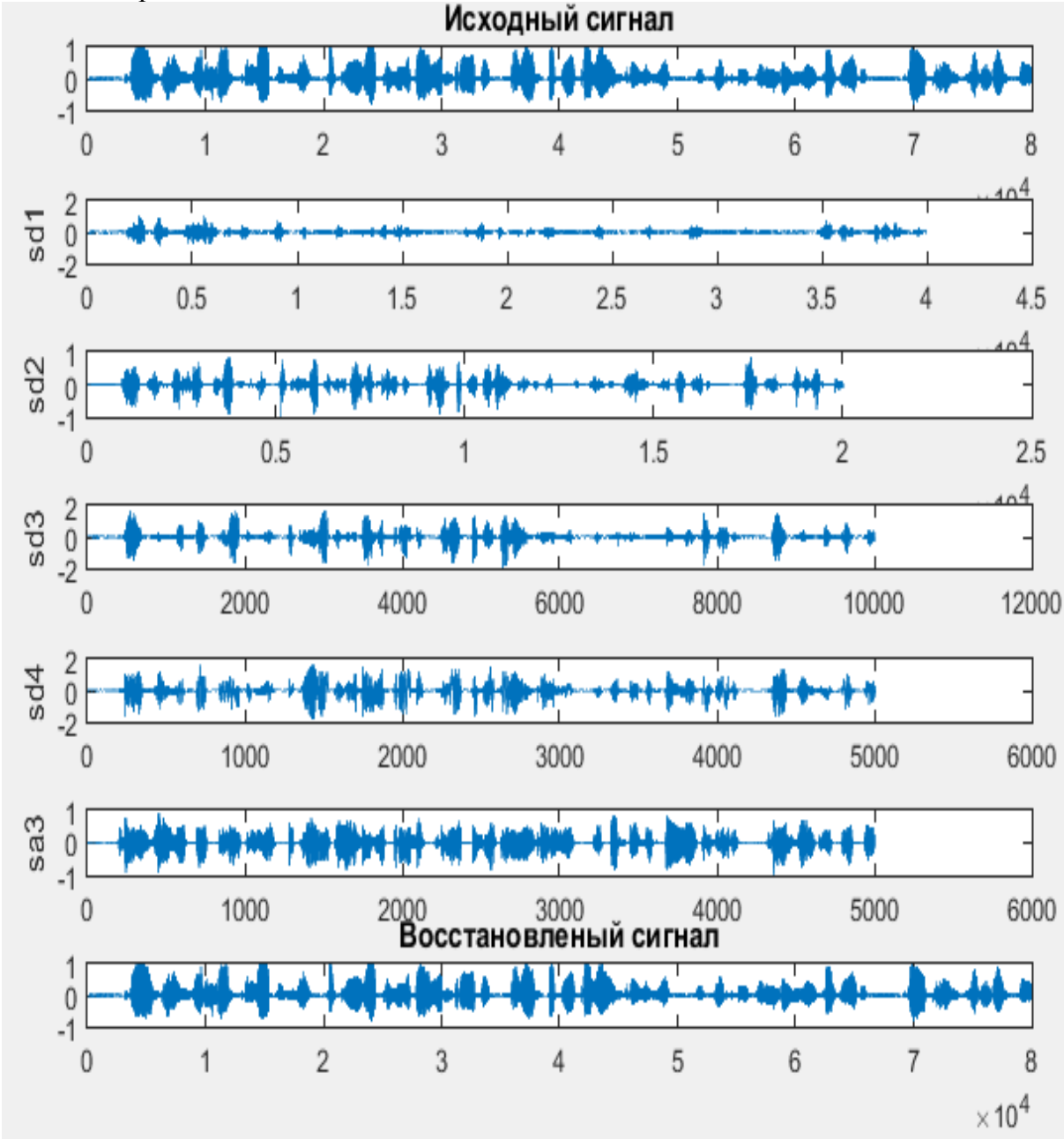


Рис.3. Быстрое вейвлет преобразование примененное к аудиосигналу

Скремблирование сигнала

Для того чтобы скрыть информацию в аудиосигнале, достаточно перемешать коэффициенты различных уровней разложения между собой по определенному алгоритму. Благодаря свойствам вейвлет-спектра подобное воздействие на вейвлет коэффициенты приведет к изменению сигнала как в частотной, так и во временной области.

В программе MatLab декомпозиция сигнала представлена в следующем виде

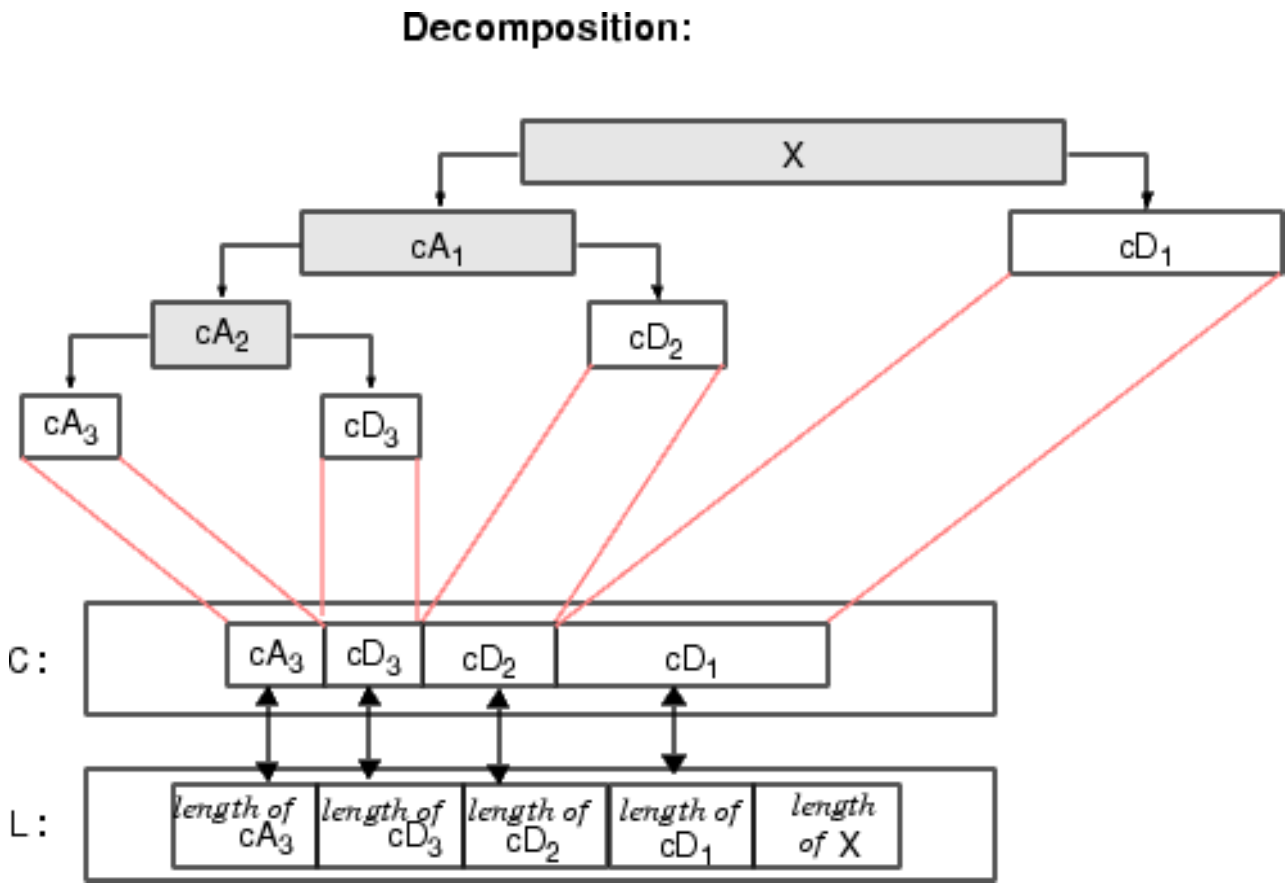


Рис.4. Результат выполнения БВП в MatLab

Как видно из рисунка на выходе имеется вектор вейвлет коэффициентов составленный из коэффициентов на всех уровнях, последовательным приписыванием каждого уровня к предыдущему начиная с минимального. Данный вид представления позволяет выполнить перемежение вейвлет коэффициентов простым переобазначением индексов массива.

В дальнейшем восстановив из перемешанного спектра сигнал, получается заскремблированные аудиоданные как в частотной так и во временной области.

Для перемежения коэффициентов спектра быстрого вейвлет преобразования и последующего восстановления скремблированного сигнала был разработан следующий код:

```
%загрузка коэффициентов load('wav_dec.mat');

for i=1:1:10000
new_dec(i)=dec(40000+i-1);% от 40000 до 50000 /10000 new_dec(10000+i)=dec(60000+i-1); % от 60000 до 70000 /20000 new_dec(20000+i)=dec(i); % от 0 до 10000 /30000
new_dec(30000+i)=dec(70000+i-1); % от 70000 до 80000 /40000
new_dec(40000+i)=dec(10000+i-1); % от 10000 до 20000 /50000
new_dec(50000+i)=dec(30000+i-1); % от 30000 до 40000 /60000
new_dec(60000+i)=dec(20000+i-1); % от 20000 до 30000 /70000
new_dec(70000+i)=dec(50000+i-1); % от 50000 до 60000 /80000 end
for i=80000:1:80026
new_dec(i)=dec(i); % от 50000 до 60000 /80000
end new_dec=new_dec';
save ScrDecomp new_dec;
% Извлечение коэффициентов разложения
```

```
new_sa4 = appcoef (new_dec, struct, wname,4); new_sd4= detcoef (new_dec, struct, 4);
new_sd3= detcoef (new_dec, struct, 3); new_sd2= detcoef (new_dec, struct, 2); new_sd1= detcoef
(new_dec, struct, 1);
% Графическая поддержка subplot (711)
plot (x1), title ('Исходный сигнал') subplot (712)
plot (new_sd1), ylabel ('sd1') subplot (713)
plot (new_sd2), ylabel ('sd2') subplot (714)
plot (new_sd3), ylabel ('sd3') subplot (715)
plot (new_sd4), ylabel ('sd4') subplot (716)
plot (new_sa4), ylabel ('sa3')
scrembl_sign = waverec (new_dec, struct, wname);
% Рисуем восстановленный сигнал subplot (717);
plot (scrembl_sign), title ('Скремблированный сигнал'); save Scr_sig scrembl_sign;
load('Record1.mat'); Voice_sound(:,1)=scrembl_sign(:,1); Voice_sound(:,2)=scrembl_sign(:,1);
player = audioplayer(Voice_sound, Fs, nBits); start = 1;
stop = player.SampleRate * nSeconds; play(player, [start stop]);
%pause(player)
%resume(player)
```

При выполнении данного кода были получены следующие результаты:

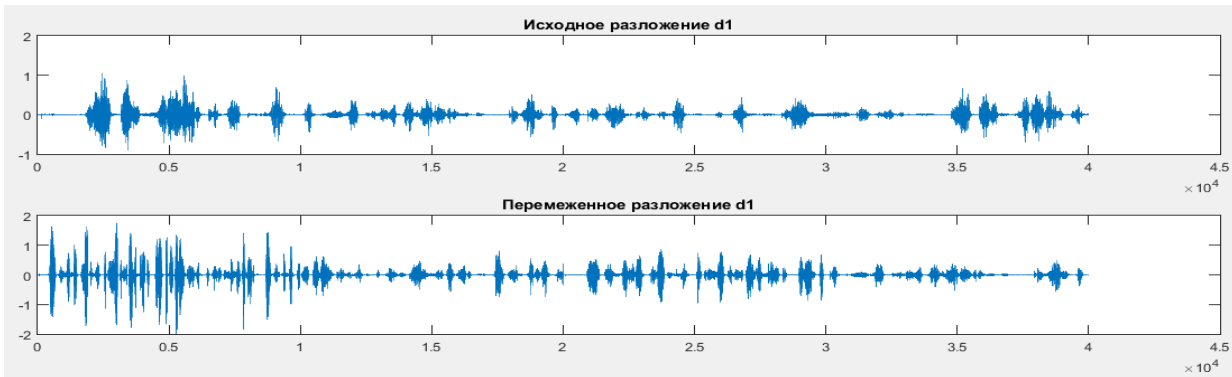


Рис. 5. Разложение на уровне d1

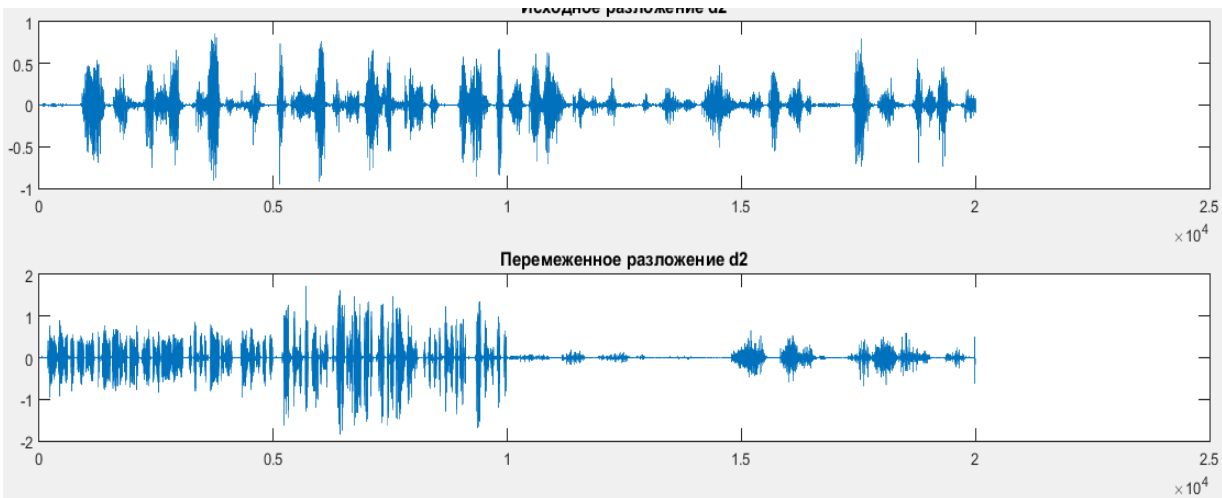


Рис.7. Разложение на уровне d3

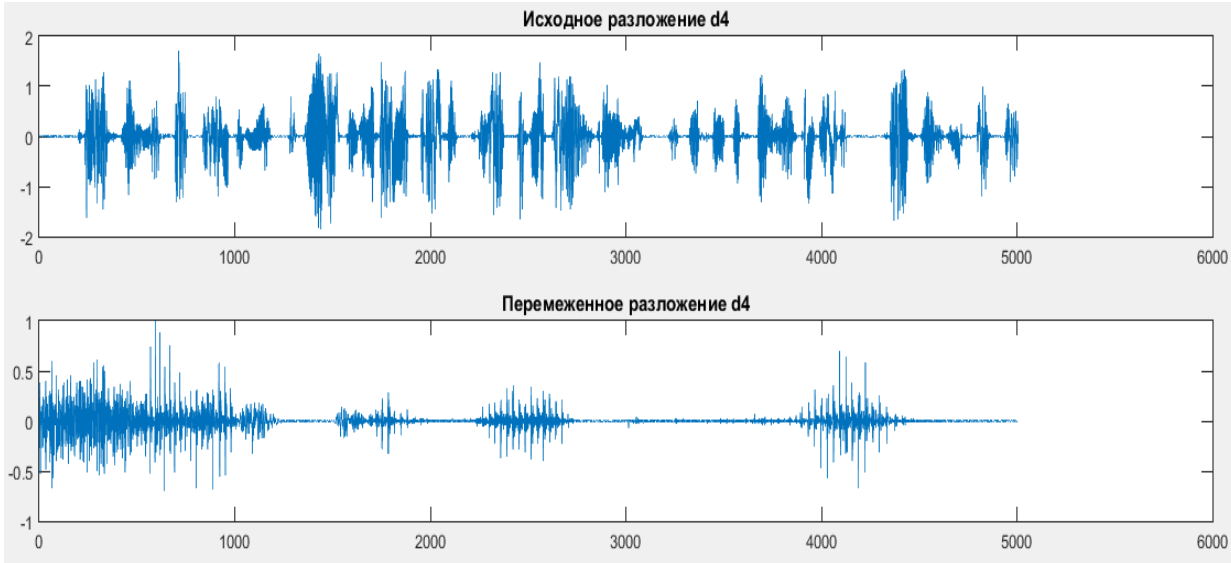


Рис.8. Разложение на уровне d4

При этом из полученный сигнал не похож на исходной в достаточной степени, чтобы говорить о защищенности информации.

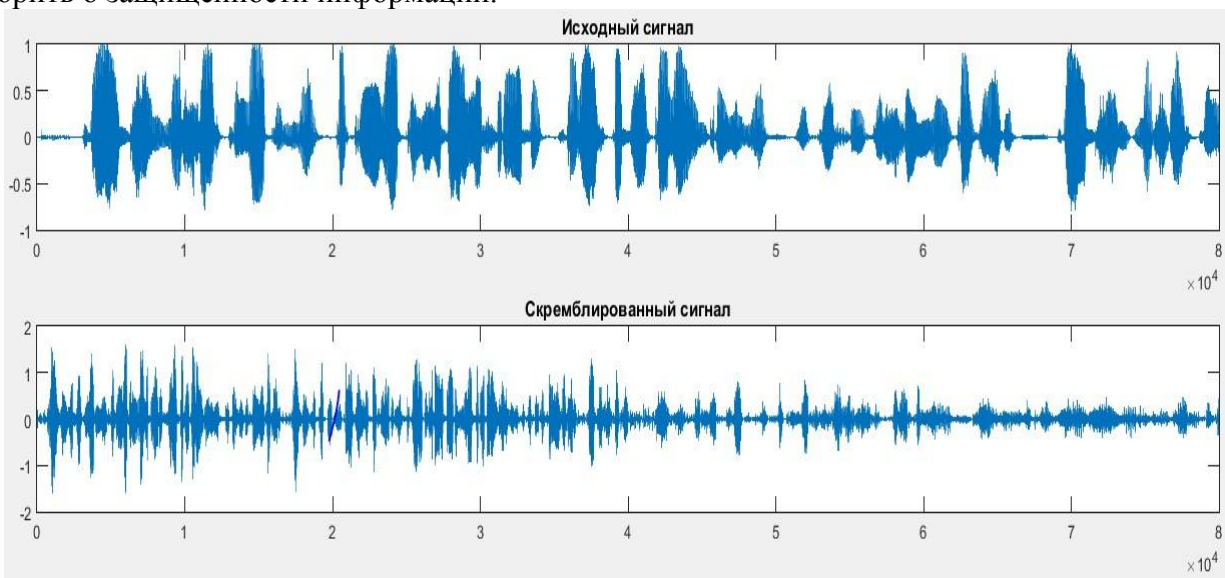


Рис. 9. Исходный и заскремблированный сигналы.

Восстановление исходного сигнала

Для восстановления исходного сигнала скремблированный сигнал подвергается быстрому вейвлет преобразованию. Полученные коэффициенты вейвлет-спектра по алгоритму, обратному скремблирующему, перемешиваются, для получения исходного спектра. На основании полученного спектра происходит восстановление сигнала. При должном навыке и практических исследованиях возможно добиться восстановления сигнала без искажений. На рисунке 10 представлен восстановленный сигнал имеющий небольшие искажения в следствии несовершенных алгоритмов перемежения спектра.

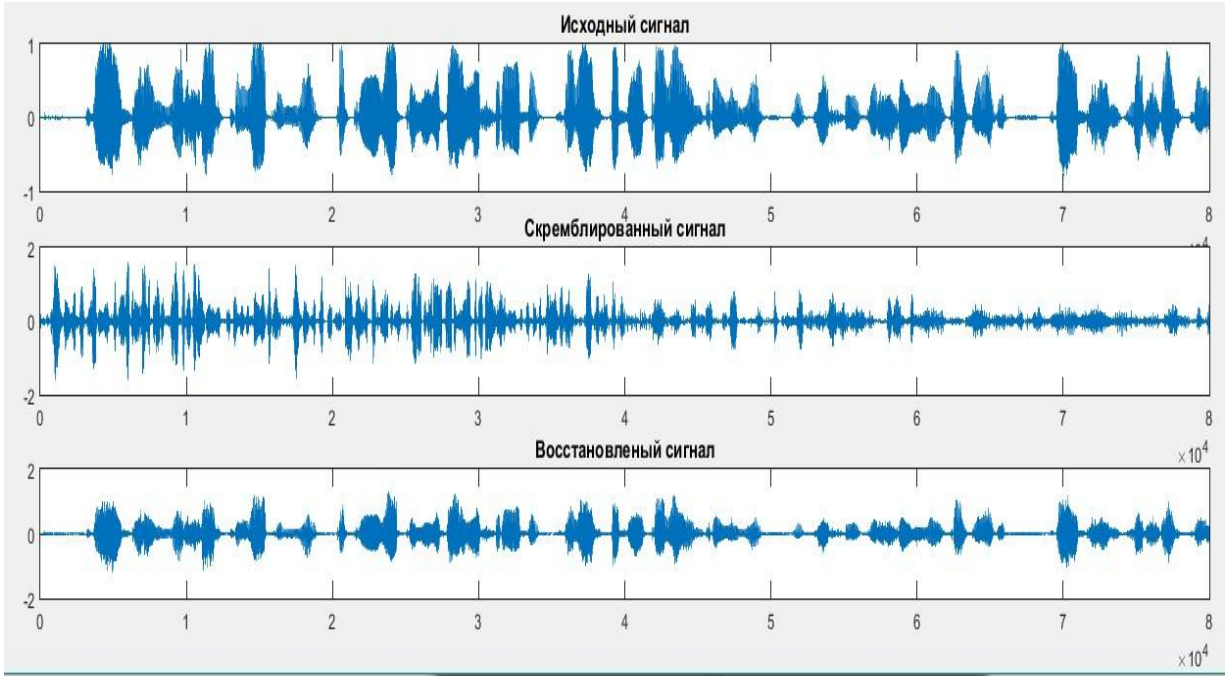


Рис.10. Исходный, заскремблированный и восстановленный сигналы На рисунке 2.11 представлено разложение на уровне d1, как видно восстановленный спектр довольно точно повторяет исходный.

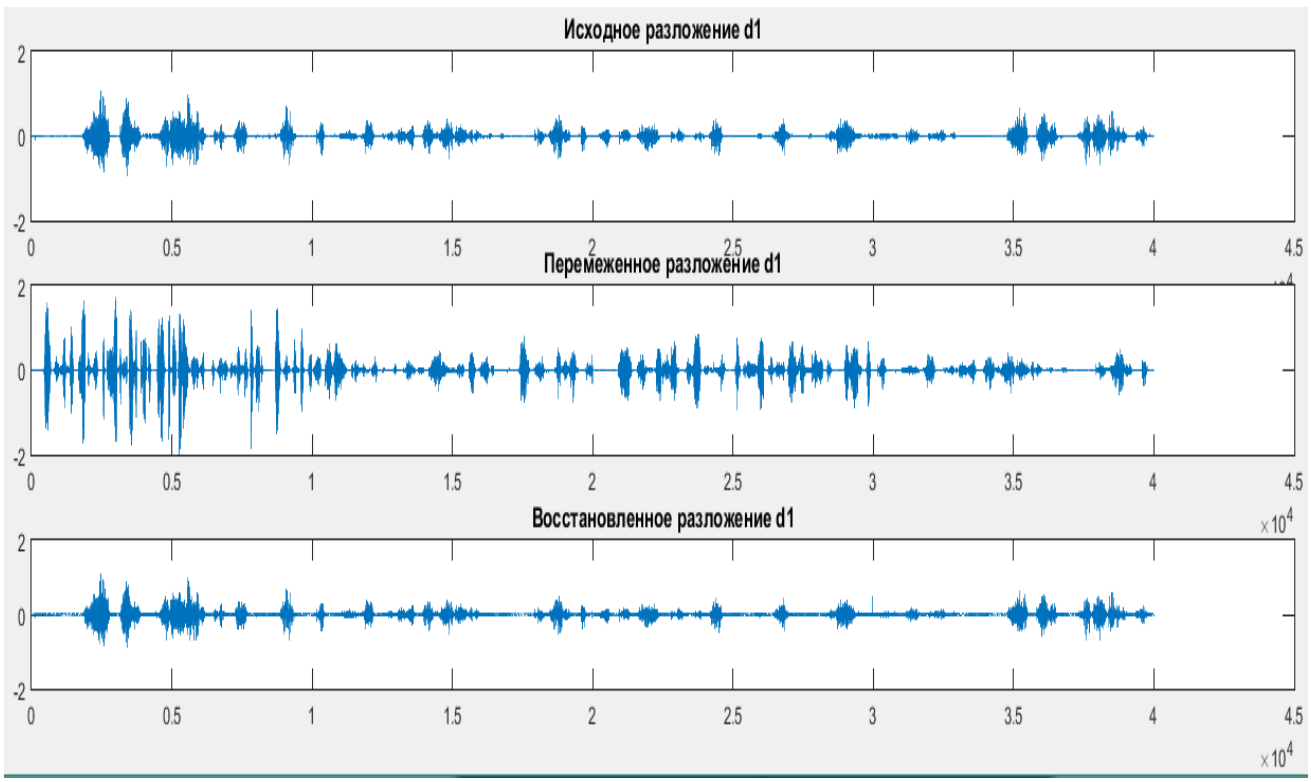


Рис. 11. Исходный, заскремблированный и восстановленный уровни разложения d1
На рисунках 12-14 изображены разложения на уровнях d2, d3 и d4 соответственно.

Рис.12. Исходный, заскремблированный и восстановленный уровни разложения d2

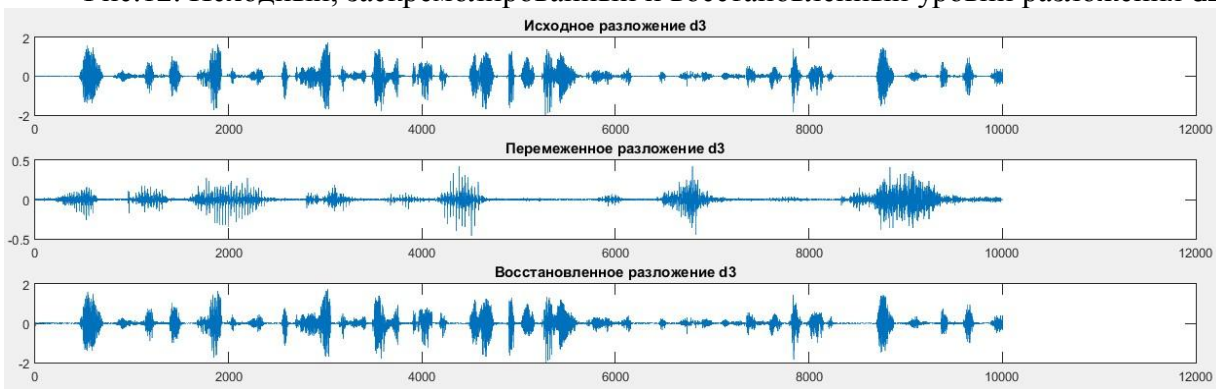


Рис. 13. Исходный, скремблированный и восстановленный уровни разложения d3

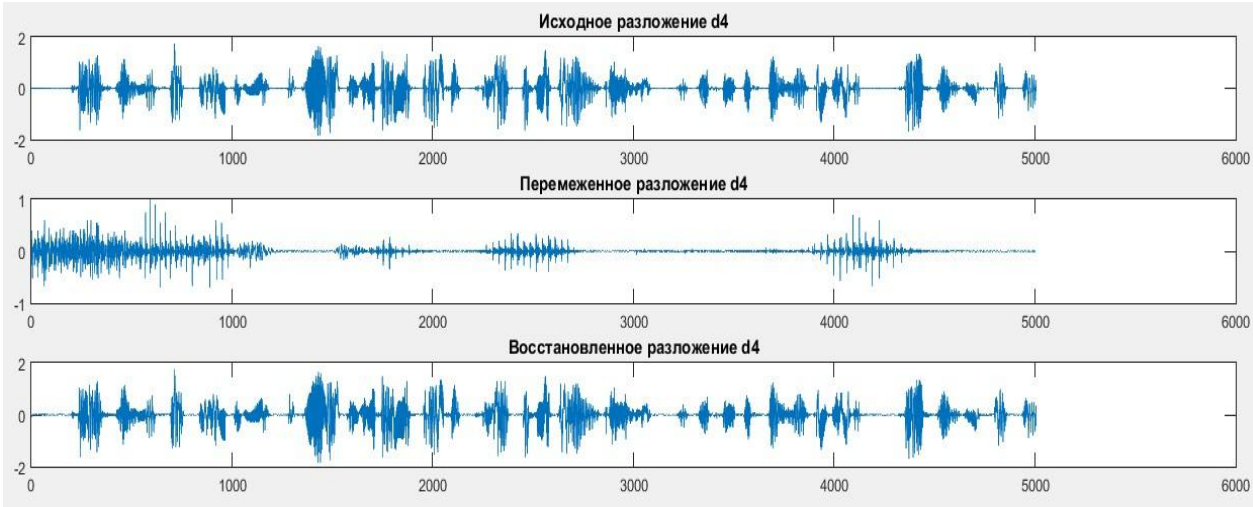


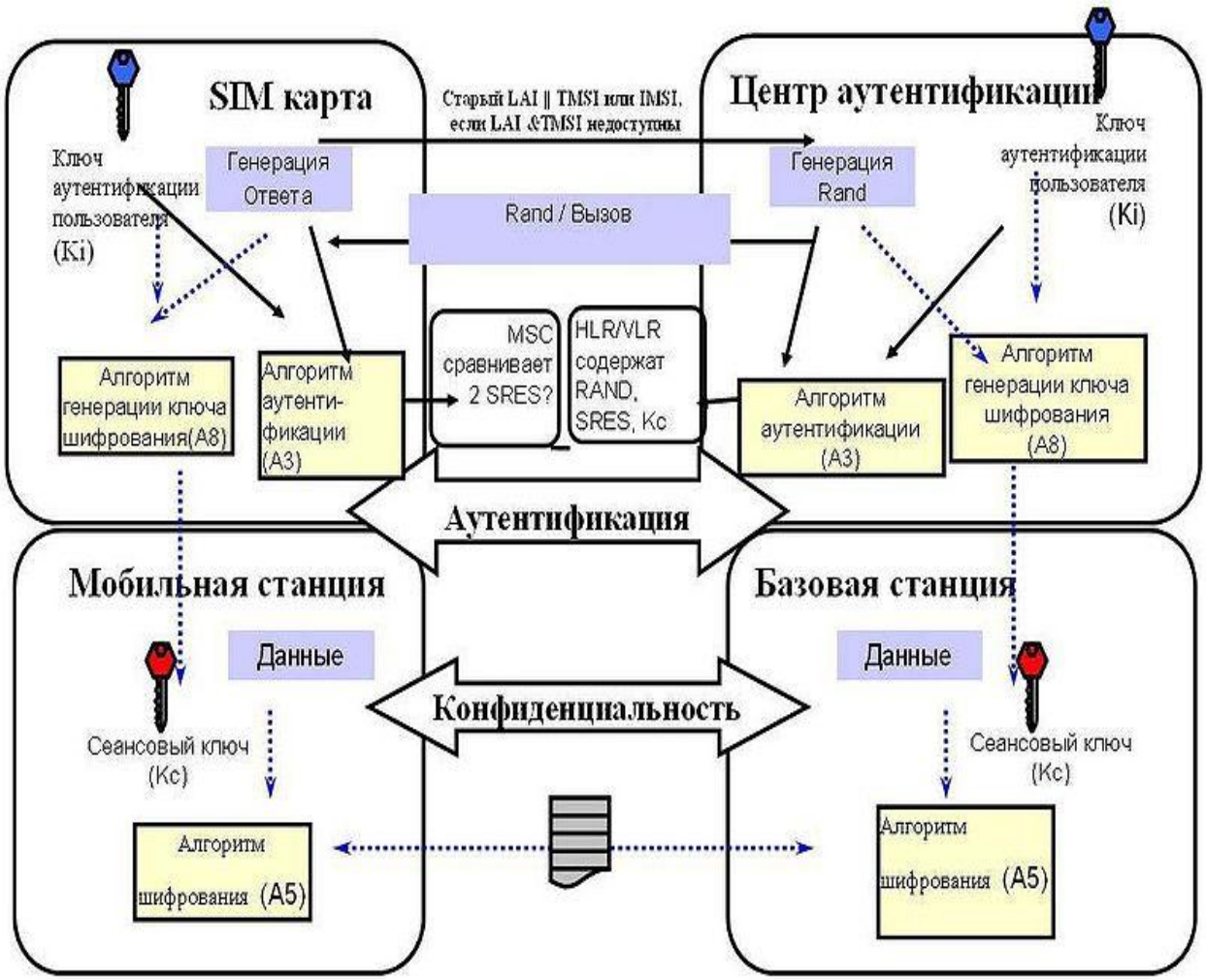
Рис.14. Исходный, скремблированный и восстановленный уровни разложения d4

В лабораторной работе исследовано скремблирование аудиосигнала с помощью вейвлет преобразования. Установлено, что вейвлет преобразование позволяет выполнить как частотное так и временное скремблирование одновременно, что повышает крипто стойкость. Восстановленный сигнал в достаточной степени соответствует исходному, при практических исследования и должном навыке возможно полное восстановление сигнала без искажений.

10. Компьютерный практикум

Задание 1. Исследование алгоритма поточного шифрования A5/1 сотовой системы связи GSM

Прежде чем приступить к описанию алгоритма шифрования используемого в GSM сетях рассмотрим каким образом происходит аутентификация пользователя и формирования ключа шифрования. Для этого воспользуемся картинкой.



На данном рисунке схематично представлены следующие шаги:
Телефон оператора подключается к сети.

1. Для подтверждения своей подлинности телефон посылает специальный идентификационный код, называемый TMSI(Temporary Mobile Subscriber Identity).
2. Центр Аутентификации(ЦА) генерирует 128-битное случайное число RAND и посылает его на Мобильную Станцию(МС).
3. МС зашифровывает полученное число RAND, используя свой секретный ключ K_i и алгоритм аутентификации A3.
4. МС берет первые 32 бита из последовательности, полученной на предыдущем шаге(назовем их SRES(signed response)) и отправляет их обратно на ЦА.
5. ЦА проделывает ту же операцию и получает 32 битную последовательность XRES(expected response).
6. После чего ЦА сравнивает SRES и XRES. В случае, если оба значения равны, телефон считается аутентифицированным.

7. МС и ЦА вычисляют сессионный ключ шифрования, используя секретный ключ K_i и алгоритм формирования ключа A8 $K_c=A8_{ki}(RAND)$

Говоря об алгоритмах аутентификации A3 и алгоритме формирования ключа A8, следует отметить что на практике большинство сотовых операторов используют для этих целей один алгоритм, называемый COMP128(он имеет множество модификаций COMP128-1, COMP128-2, COMP128-3).
COMP128 представляет собой обыкновенную хэш-функцию, на входе которая принимает 128-битную последовательность и на выходе возвращает 96-битную.

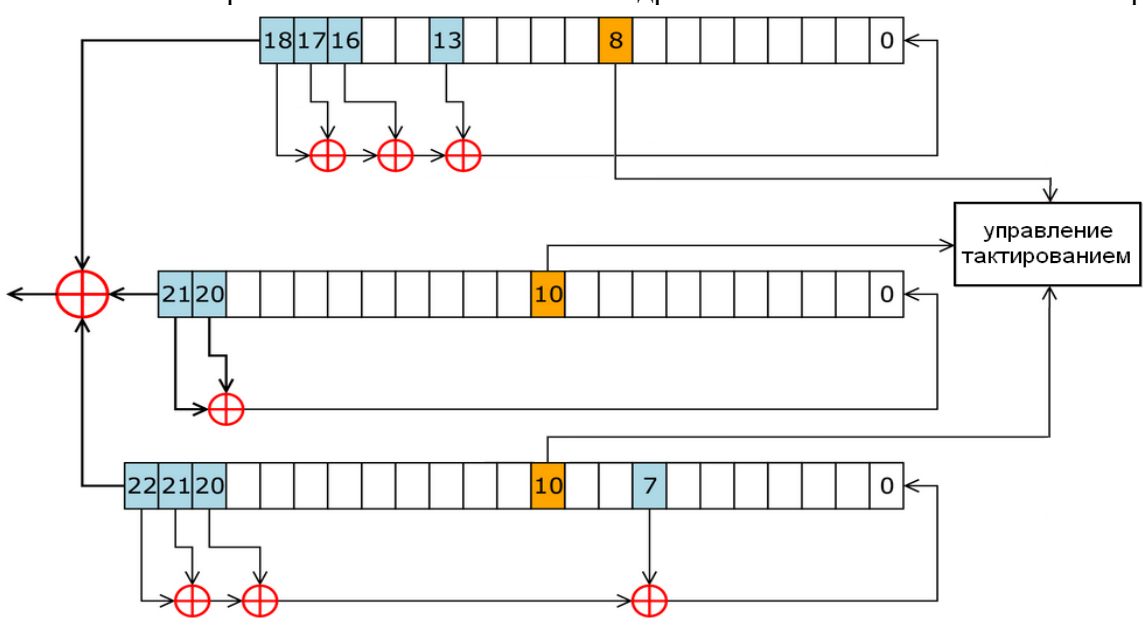
Как всегда в криптографии, попытка сэкономить время разработчикам обернулась полным провалом. Безопасность GSM сетей изначально основывалась на принципе «безопасность за счёт неизвестности». И когда в 1998 году алгоритм был вскрыт группой исследователей состоящих из Marc Briceno, Ian Goldberg и David Wagner обранужилась одна занятная особенность: последние 10 бит секретного ключа K_i всегда равнялись нулю. Используя это любопытное свойство, а так же уязвимость COMP128 к «атаке дней рождений» Marc Briceno, Ian Goldberg и David Wagner смогли извлечь секретный ключ K_i из SIM-карты.
Результатом этого исследования стал повсеместный отказ от алгоритма COMP128 и его замена на более надежные модификации COMP128-2 и COMP128-3, технические детали которых держатся в тайне.

Алгоритм шифрования A5/1

В качестве алгоритма шифрования в GSM используются алгоритмы из семейства A5. На сегодняшний день их всего 3:

A5/1 — поточный шифр, наиболее распространенный на сегодня.

- **A5/2**-вариант предыдущего алгоритма «для бедных». Очень похож на своего «старшего брата», но изначально задумывался, как сильно ослабленная версия A5/1. В настоящее время не используется
- **A5/3**-блочный шифр. Разработан в 2002 году с целью заменить устаревший A5/1. Однако в настоящее время используется только в 3GPP сетях. У алгоритма найден ряд уязвимостей, но о практических атаках речи пока не идет.
- Рассмотрим подробнее алгоритм



A5/1.

Внутреннее состояние шифра A5/1 состоит из трех линейных регистров сдвига с обратной связью R1, R2, R3, длиной 19, 22 и 23 бита соответственно(всего 64 бита).

Сдвиг в регистрах R1, R2, R3 происходит только при выполнении определенного условия. Каждый регистр содержит " бит управления тактированием". В R1 это 8-й бит, а в R2 и R3 — 10-й. На каждом шаге сдвигаются только те регистры у которых значение бита синхронизации равно большинству значений синхронизирующих битов всех трех регистров.

На сегодняшний день известно большое количество успешных атак на GSM шифрование и все они относятся к атакам типа known-plaintext, т.е. для восстановления ключа атакующему помимо зашифрованных фреймов необходимо знать так же незашифрованные данные, которые соответствуют этим фреймам. На первый взгляд такое требование может показаться фантастическим, однако из-за специфики стандарта GSM, в котором помимо голосового трафика передаются различные системные сообщения, такого рода атаки из разряда теоретических переходят в разряд практических.

Системные сообщения GSM содержат повторяющиеся данные и могут использоваться злоумышленником. В частности метод, предложенный Karsten Nohl в 2010 году основан как раз таки на поиске такого рода данных в шифротексте и простом переборе различных вариантов ключей, хранящихся в радужных таблицах, до тех пор пока не будет найден ключ, порождающий нужный шифротекст для известного заранее системного сообщения.

Задание 2.Криптографическая защита беспроводной сети LTE

Стандарт сетей LTE [16] – стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и других терминалов, работающих с данными. Он основан на GSM/EDGE и UMTS/HSPA сетевых технологиях, увеличивая пропускную способность и скорость за счёт использования другого радиоинтерфейса вместе с улучшением ядра сети.

На рисунке 5.1 представлена структура сети стандарта LTE.

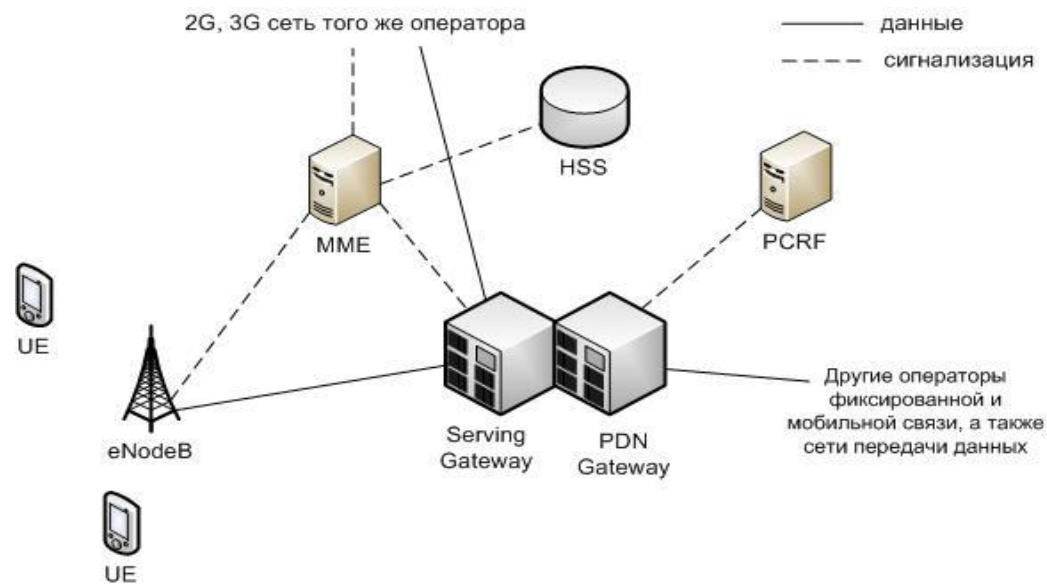


Рис. 10.1. Структура сети стандарта LTE

Из этой схемы видно, что структура сети сильно отличается от сетей стандартов 2G и 3G. Существенные изменения претерпела и подсистема базовых станций, и подсистема

коммутации. Изменена технология передачи данных между оборудованием пользователя и базовой станцией. Также подверглись изменению и протоколы передачи данных между сетевыми элементами. Вся информация (голос, данные) передается в виде пакетов. Таким образом, уже нет разделения на части обрабатывающие либо только голосовую информацию, либо только пакетные данные.

Можно выделить следующие основные элементы сети стандарта LTE:

- **Serving SAE Gateway** или просто **Serving Gateway** *(SGW)* – обслуживающий шлюз сети LTE. Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. SGW имеет прямое соединение с сетями второго и третьего поколений того же оператора, что упрощает передачу соединения в /из них по причинам ухудшения зоны покрытия, перегрузок и т.п. В SGW нет функции коммутации каналов для голосовых соединений, т.к. в LTE вся информация, включая голос коммутируется и передается с помощью пакетов.
- **Public Data Network SAE Gateway** или просто **PDN Gateway** *(PGW)* – шлюз к сетям передачи данных других операторов для сети LTE. Основная задача PGW заключается в маршрутизации трафика сети LTE к другим сетям передачи данных, таких как Интернет, а также сетям GSM, UMTS.
- **Mobility Management Entity** *(MME)* – узел управления мобильностью сети сотовой связи стандарта LTE. Предназначен для обработки сигнализации, преимущественно связанной с управлением мобильностью абонентов в сети.
- **Home Subscriber Server** *(HSS)* – сервер абонентских данных сети сотовой связи стандарта LTE. Представляет собой большую базу данных и предназначен для хранения данных об абонентах. Кроме того, HSS генерирует данные, необходимые для осуществления процедур шифрования, аутентификации и т.п. Сеть LTE может включать один или несколько HSS. Количество HSS зависит от географической структуры сети и числа абонентов.
- **Policy and Charging Rules Function** *(PCRF)* – элемент сети сотовой связи стандарта LTE, отвечающий за управление начислением платы за оказанные услуги связи, а также за качество соединений в соответствии с заданными конкретному абоненту характеристиками.

Для того чтобы данные могли быть транспортированы через интерфейс радио LTE, используются различные «каналы». Они используются для того, чтобы выделять различные типы данных и позволить им транспортироваться через сеть доступа более эффективно. Использование нескольких каналов обеспечивает интерфейс более высокого уровня в рамках протокола LTE и включают более чёткую и определенную сегрегацию данных.

Есть три категории, в которые могут быть сгруппированы различные каналы передачи данных:

Логические каналы – предоставляет услуги среднего уровня управления доступом MAC *(Medium Access Control)* в пределах структуры протокола LTE. Логические каналы по типу передаваемой информации делятся на логические каналы управления и логические каналы трафика. Логические каналы управления используются для передачи различных сигнальных и информационных сообщений. По логическим каналам трафика передают пользовательские данные.

Транспортные каналы — транспортные каналы физического уровня предлагают передачу информации в MAC и выше. Информацию логических каналов после обработки на RLC/MAC уровнях размещают в транспортных каналах для дальнейшей передачи по радиоинтерфейсу в физических каналах. Транспортный канал определяет как и с какими характеристиками происходит передача информации по радиоинтерфейсу. Информационные сообщения на транспортном уровне разбивают на транспортные блоки. В каждом временном интервале передачи (Transmission Time Interval, TTI) по

радиоинтерфейсу передают хотя бы один транспортный блок. При использовании технологии MIMO возможна передача до четырех блоков в одном TTI.

Физические каналы – это каналы передачи, которые переносят пользовательские данные и управляющие сообщения. Они изменяются между восходящим и нисходящим потоками, поскольку каждый из них имеет различные требования и действует по-своему.

Существующие методы и стандарты защиты беспроводных сетей LTE

Безопасность в сетях LTE заключается в нескольких видах:

- Защита абонентов.
- Защита передаваемых сообщений.
- Шифрование сообщений.
- Аутентификация и абонента, и сети.

Защита абонента заключается в том, что в процессе обслуживания его скрывают временными идентификаторами.

Для закрытия данных в сетях LTE используется потоковое шифрование методом наложения на открытую информацию псевдослучайной последовательности (ПСП) с помощью оператора XOR (исключающее или). В этих сетях для обеспечения безопасности внутри сети применяется принцип туннелирования соединений. Шифрации можно подвергать пакеты S1 и X2 при помощи IPsec ESP, а также подвергаются шифрации сигнальные сообщения этих интерфейсов.

В момент подключения или активизации абонентского оборудования (UE) в сети, сеть запускает процедуру аутентификации и соглашения о ключах AKA (Authentication and Key Agreement). Целью этой процедуры является взаимная аутентификация абонента и сети и выработка промежуточного ключа K_{ASME}. Работа механизма AKA занимает доли секунды, которые необходимы для выработки ключа в приложении USIM и для установления соединения с Центром регистрации (HSS). Вследствие этого, для достижения скорости передачи данных сетей LTE необходимо добавить функцию обновления ключевой информации без инициализации механизма AKA. Для решения этой проблемы в сетях LTE предлагается использовать иерархическую ключевую инфраструктуру. Здесь также, как и в сетях 3G, приложение USIM и Центр аутентификации (AuC) осуществляет предварительное распределение ключей. Когда механизм AKA инициализируется для осуществления двусторонней аутентификации пользователя и сети, генерируются ключ шифрования CK и ключ общей защиты, которые затем передаются из ПО USIM в Мобильное оборудование (ME) и из Центра аутентификации в Центр регистрации (HSS). ME и HSS, используя ключевую пару (CK;IK) и ID используемой сети, вырабатывает ключ K_{ASME}. Установив зависимость ключа от ID сети, Центр регистрации гарантирует возможность использования ключа только в рамках этой сети. Далее K_{ASME} передается из Центра регистрации в устройство мобильного управления (MME) текущей сети, где он используется в качестве мастер-ключа. На основании K_{ASME} вырабатывается ключ $K_{nas\text{-}enc}$, который необходим для шифрования данных протокола NAS между мобильным устройством (UE) и MME, и $K_{nas\text{-}int}$, необходимый для защиты целостности. Когда UE подключается к сети, MME генерирует ключ KeNB и передает его базовым станциям. В свою очередь, из ключа KeNB вырабатывается ключ Kup-enc, используемый для шифрования пользовательских данных протокола U-Plane, ключ Krrc-enc для протокола RRC (Radio Resource Control - протокол взаимодействия между Мобильными устройствами и базовыми станциями) и ключ Krrc-int, предназначенный для защиты целостности.

Алгоритм аутентификации и генерации ключа представлен на рис 10.2

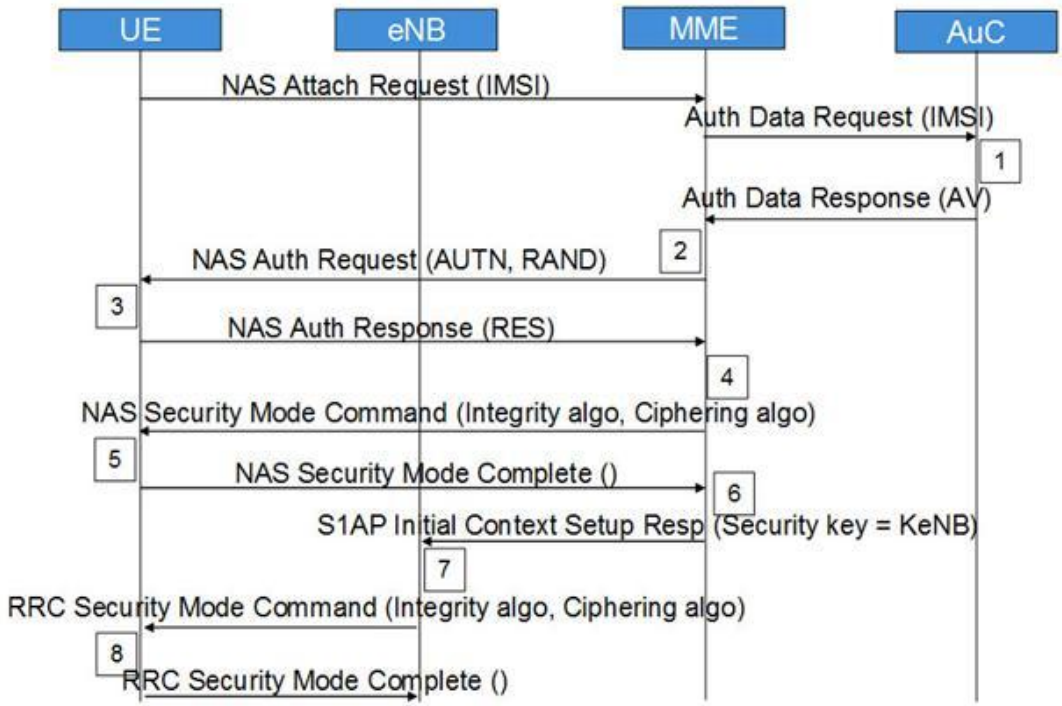


Рис. 10.2. Алгоритм аутентификации и генерации ключа

Здесь:

Шаг 1. Запрос о подключении к сети от мобильной станции (UE). MME запрашивает аутентификационные данные, относящиеся к конкретному IMSI, отправляя Authentication Data Request. AuC/HSS выбирает PSK, относящийся к конкретному IMSI и вычисляет аутентификационные данные по PSK. AuC/HSS отправляет обратно AV с Authentication Data Response.

Шаг 2. MME получает IK, CK, XRES, RAND и AUTH из AV. MME отправляет AUTH и RAND при помощи Authentication Request к UE.

Шаг 3. UE аутентифицирует NW, проверяя полученный AUTH. После чего вычисляет IK, CK, RES, XMAC из своего ключа защиты, AMF, (OP), AUTH и RAND. Она отправляет RES с Authentication response.

Шаг 4. После получения RES, MME сравнивает его с XRES и если они совпадают, то аутентификация прошла успешно, в противном случае, MME отправляет сбой аутентификации (Authentication failure) к UE. MME сбрасывает счетчик DL NAS. Рассчитывает KASME, KeNB, Knas-int, Knas-enc. Отправляет NAS команду режима безопасности (алгоритм целостности, алгоритм шифрования, NAS набор ключей ID, функцию безопасности UE) с целостностью охраняемых, но не зашифрованных, используя Knas-inc.

Шаг 5. После получения NAS команды режима безопасности, UE вычисляет KASME, KeNB, Knas-int, Knas-enc. UE отправляет NAS режима безопасности выполнен с целостностью, защищенных и зашифрованных.

Шаг 6. После получения NAS команды режима безопасности от UE, MME отправляет KeNB в eNB с S1AP первоначальная установка начального контекста (ключ защиты).

Шаг 7. После получения KeNB, eNB вычисляет Krrc-int, Krrc-enc, Kup-enc. Затем оно отправляет RRC ключ защиты команду с AS целостностью алгоритма и AS шифрующий алгоритм.

Шаг 8. После получения RRC команды ключа защиты UE вычисляет Krrc-int, Krrc-enc, Kup-enc. UE отправляет RRC выполненный ключ шифрования на eNB.

После всех описанных действий, все NAS и AS сообщения будут надежно защищены и зашифрованы, в отличие от пользовательских данных, которые будут только шифроваться.

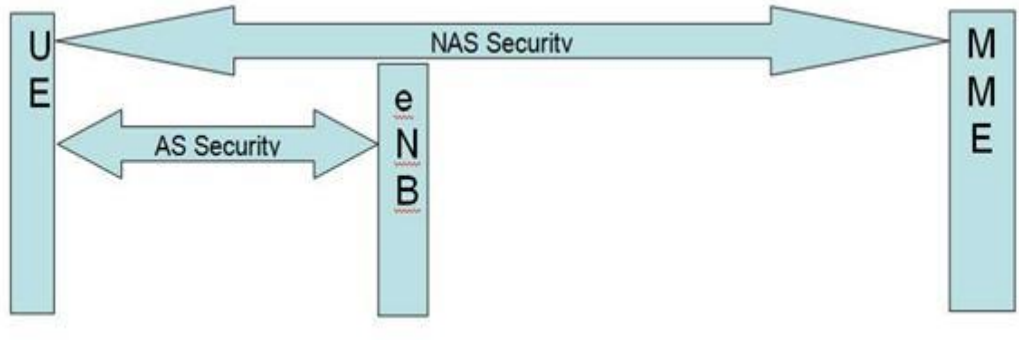


Рис. 10.3. Слои безопасности

Архитектура безопасности LTE определяет механизм безопасности и для уровня NAS и для уровня AS.

Безопасность NAS (слоя без доступа): Выполнена для NAS сообщений и принадлежит области UE и MME.

В этом случае необходима при передаче сообщений NAS между UE и MME – целостность, защищенная и зашифрованная с дополнительным заголовком безопасности NAS.

Безопасность AS (слоя с доступом): Выполнена для RRC и плоскости пользовательских данных, принадлежащих области UE и eNB. Уровень PDCP на сторонах UE и eNB отвечает за шифрование и защиту целостности.

RRC сообщения защищены целостностью и зашифрованы, однако данные U-Plane только зашифрованы.

Для генерации векторов аутентификации используется криптографический алгоритм с помощью однонаправленных функций (f1, f2, f3, f4, f5) когда прямой результат получается путем простых вычислений, а обратный результат не может быть получен обратным путем, то есть не существует эффективного алгоритма получения обратного результата. Для этого алгоритма используется случайное 128 битное случайное число RAND, мастер-ключ K абонента, также 128 бит и порядковый номер процедуры SQN (Sequence Number). Счетчик SQN меняет свое значение при каждой генерации вектора аутентификации. Похожий счетчик SQN работает и в USIM. Такой метод позволяет генерировать каждый раз новый вектор аутентификации, не повторяя предыдущий уже использованный вектор аутентификации.

Помимо этих трех исходных величин: SQN, RAND и K в алгоритме f1 участвует поле управления аутентификацией Authentication Management Field (AMF), а в алгоритмах f2 – f5 исходные параметры – RAND и K, что и продемонстрировано на рис. 2.3, 2.4. На выходах соответствующих функций получают Message Authentication Code (MAC) - 64 бита; XRES – eXpected Response, результат работы алгоритма аутентификации <32 – 128 бит>; ключ шифрации CK, генерируемый с использованием входящих (K,RAND)->f3->CK; ключ целостности IK, сгенерированный с использованием входящего (K,RAND)->f4->IK; и промежуточный ключ Anonymity Key (AK), генерируемый с помощью (K,RAND)->f5->AK - 64 бита.

При обслуживании абонента сетью E-UTRAN ключи CK и IK в открытом виде в ядро сети не передают. В этом случае HSS генерирует K_{ASME} с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются CK и IK, а также идентификатор обслуживающей сети и SQNÅAK. Вектор аутентификации содержит RAND,

XRES, AUTN и K_{ASME}, на основе которого происходит генерация ключей шифрации и целостности, используемых в соответствующих алгоритмах.

Когда мобильная станция получает из ядра сети три параметра (RAND, AUTN и KSI_{ASME}, где KSI – Key Set Identifier, индикатор установленного ключа, однозначно связанный с K_{ASME} в мобильной станции).

После чего используя RAND и AUTN, USIM на основе алгоритмов безопасности, тождественных хранящимся в HSS, производит вычисление XMAC, RES, CK и IK.

Затем в ответе RES UE передает в MME вычисленное RES, которое должно совпасть с XRES, полученным из HSS. Так сеть аутентифицирует абонента. Вычислив XMAC, UE сравнивает его с MAC, полученным ею в AUTN. При успешной аутентификации абонентом сети (MAC = XMAC) UE сообщает об этом в ответе RES. Если аутентификация сети не удалась (MAC ≠ XMAC), то UE направляет в MME ответ CAUSE, где указывает причину неудачи аутентификации.

При успешном завершении предыдущего этапа MME, eNB и UE производят генерацию ключей, используемых для шифрации и проверки целостности получаемых сообщений. В E-UTRAN имеется иерархия ключей, которая приведена на рис. 2.5.

Векторы аутентификации (рис. 2.3, 2.4):

Ключи IK и CK генерируются и в центре аутентификации, и в USIM;

Ключ AK генерируется только в центре аутентификации;

Ответ XRES генерируется только в центре аутентификации, а RES генерируется в USIM;

Код MAC генерируется только в центре аутентификации, а соответствующий ему параметр XMAC генерируется в USIM;

Маркер AUTH генерируется только в центре аутентификации.

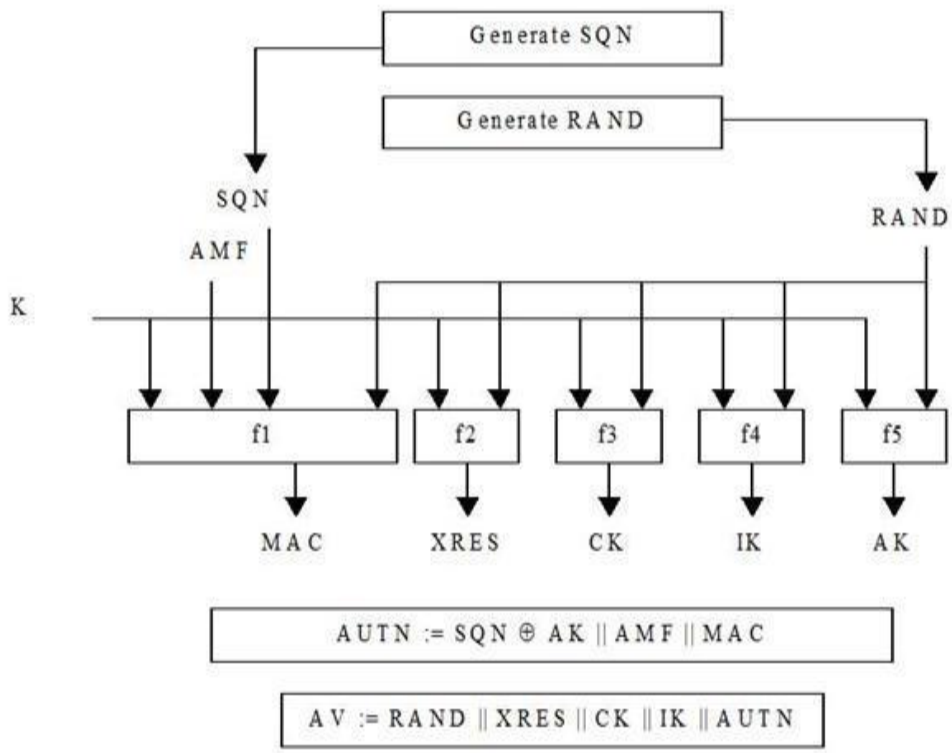


Рис. 10.4. Создание векторов на передающей стороне

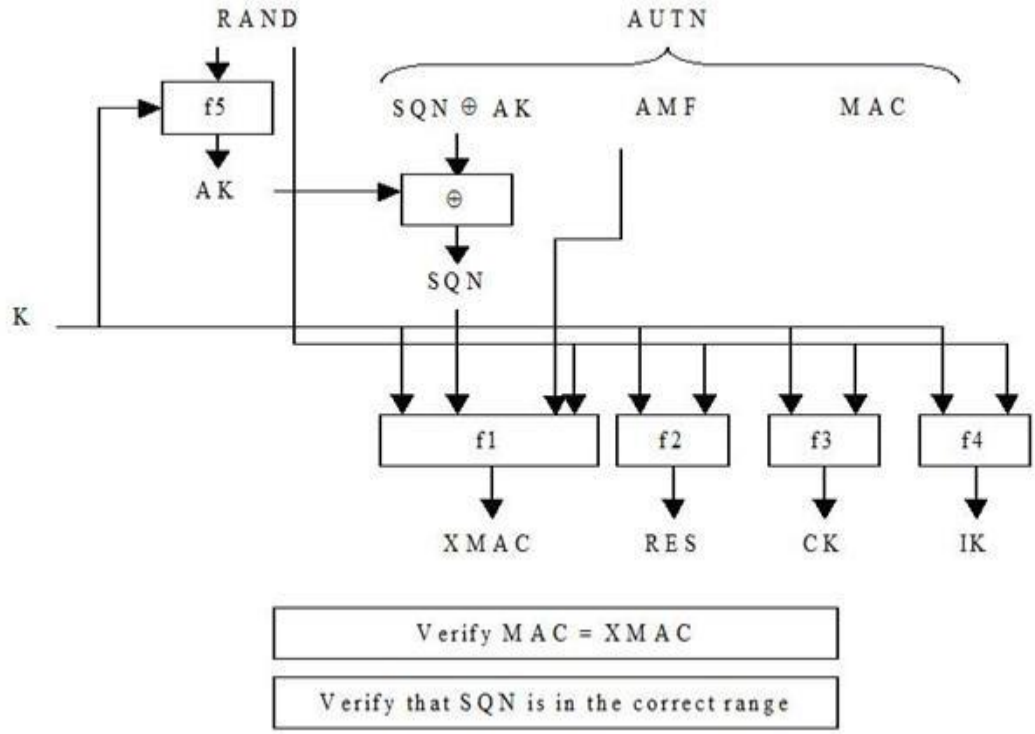


Рис. 10.5. Преобразование векторов на принимаемой стороне

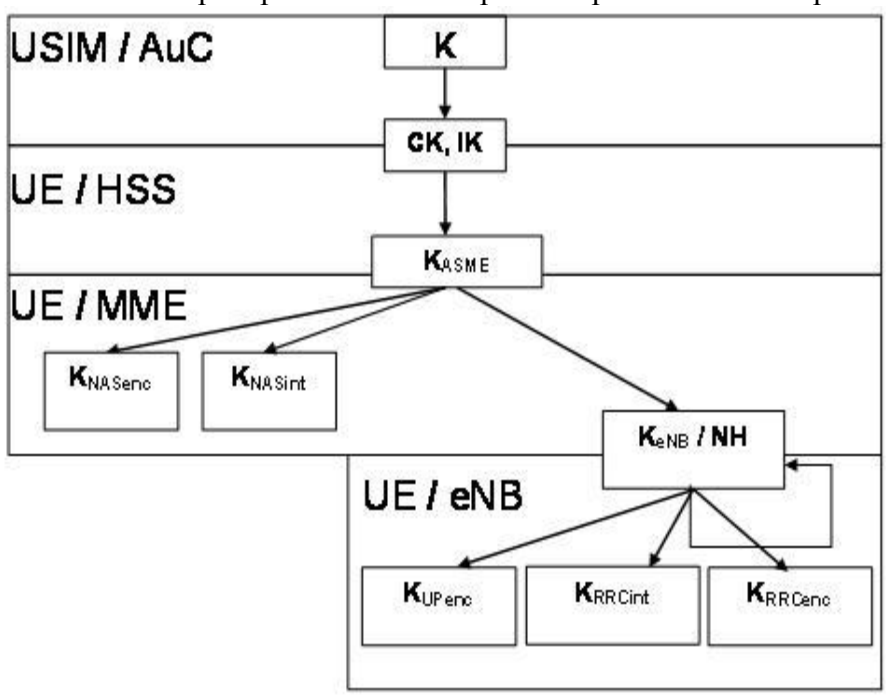


Рис. 10.6. Иерархия ключей в E-UTRAN

Исходным ключом для всей цепочки является K_{ASME} (256 бит). При передаче в радиоканале защиту обеспечивают для сигнального трафика (Control Plane) и для пользовательских пакетов (User Plane). При этом все сообщения сигнализации разделяют на сквозные сигнальные сообщения между UE и MME протоколов MM и SM (NAS – Non Access Stratum) и сигнальные сообщения между eNB протокола RRC (AS – Access Stratum). Для шифрации и защиты целостности можно использовать разные базовые алгоритмы:

- UEA2 (UMTS Encryption Algorithm 2) и UIA2 (UMTS Integrity Algorithm 2);

- разработанные для стандартов 3G,AES (Advanced Encryption Standard).

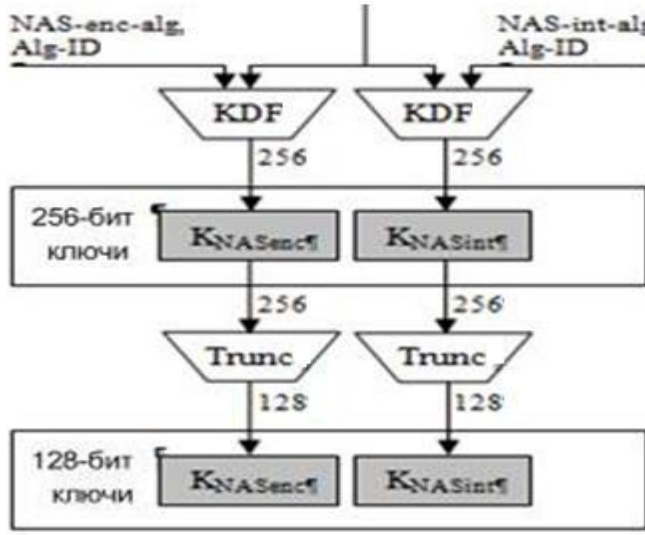


Рис. 10.7. Генерирование ключей шифрации и целостности для NAS сигнализации

Сигнальные сообщения протокола RRC (AS) также шифруют и обеспечивают их целостность. Пакеты трафика только шифруют. Эти операции производят в обслуживающей eNB и UE. Схема получения ключей шифрации и целостности (рис. 7) для AS и UP трафика отличается от предыдущего случая тем, что исходным параметром здесь служит вторичный промежуточный ключ KeNB (256 бит). Этот ключ генерируют, также используя KDF, где входными параметрами являются: KASME, счетчик сигнальных сообщений NAS вверх, прежнее значение KeNB, идентификатор соты и номер частотного канала в направлении вверх. Следовательно, при каждой периодической локализации UE происходит изменение KeNB.

Также KeNB меняется и при хэндовере; при этом в алгоритме генерации нового KeNB можно использовать дополнительный параметр NH (Next Hop), фактически счетчик числа базовых станций, по цепочке обслуживающих абонента. Все реализуемые процедуры безопасности в сети E-UTRAN продемонстрированы на рис. 2.8.

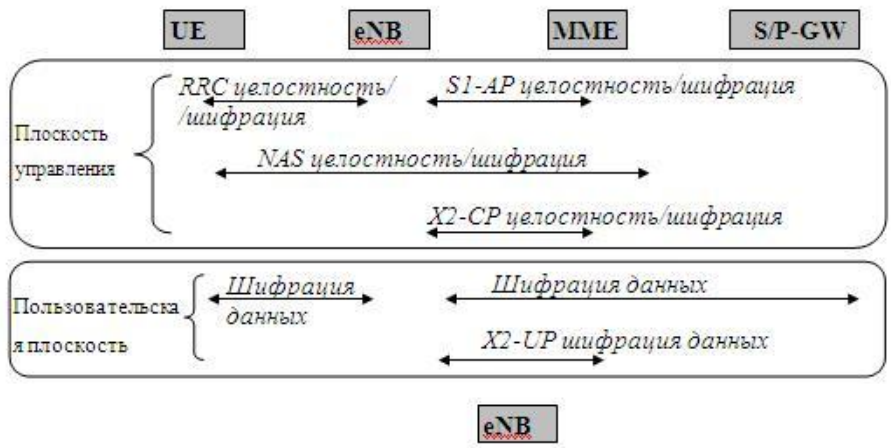


Рис. 10.8. Реализуемые процедуры безопасности в сети E-UTRAN

Алгоритм шифрации и дешифрации сообщений представлен на рис. 2.9.

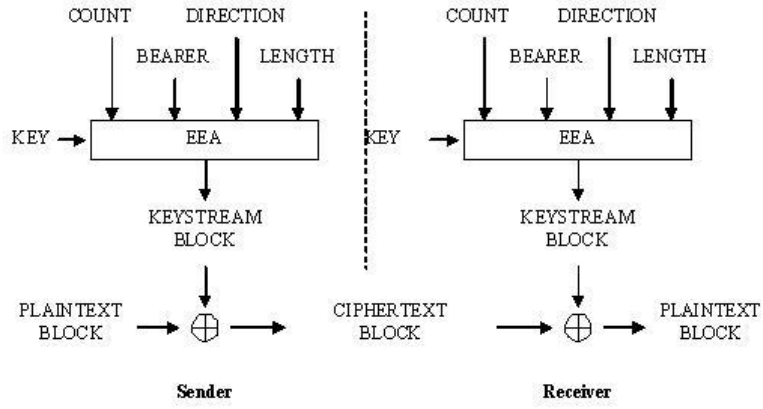


Рис. 10.9. Алгоритм шифрации в E-UTRAN

Исходными параметрами в этом алгоритме являются шифрующий ключ KEY (128 бит), счетчик пакетов (блоков) COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и длина шифрующего ключа LENGTH. В соответствии с выбранным алгоритмом шифрации EEA (EPS Encryption Algorithm) вырабатывается шифрующее число KEYSTREAM BLOCK, которое при передаче складывают по модулю два с шифруемым исходным текстом блока PLAINTEXT BLOCK. При дешифрации на приемном конце повторно совершают эту же операцию.

Процедура защиты целостности сообщения состоит в генерации “хвоста“ MAC (Message Authentication Code) (32 бита), присоединяемого к передаваемому пакету. Алгоритм генерации MAC и проверки целостности полученного пакета путем сравнения XMAC с MAC (они должны совпасть) отображен на рис. 5.10.

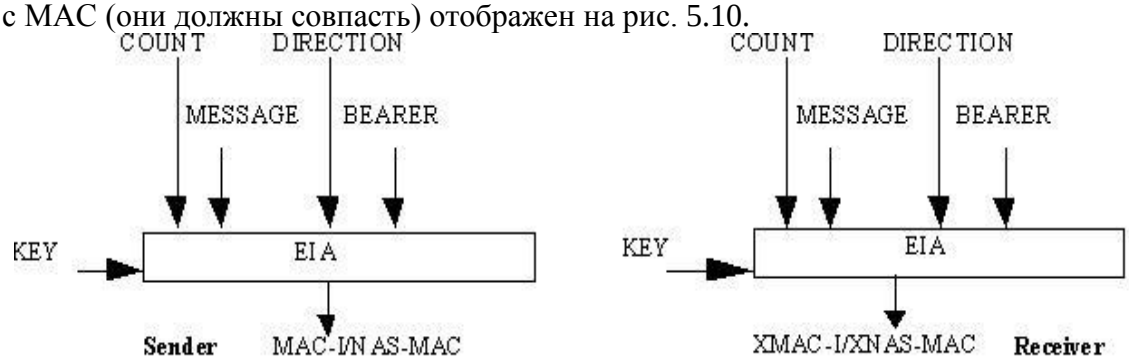


Рис. 10.10. Алгоритм проверки целостности E-UTRAN

В алгоритме EIA (EPS Integrity Algorithm) использован ключ целостности KEY (128 бит), счетчик сообщений COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и само сообщение MESSAGE.

Моделирование технологии LTE в среде MATLAB с использованием встроенного пакета LTE System Toolbox

LTE System Toolbox™ предоставляет соответствующие стандарту функции и приложения для проектирования, моделирования и проверки коммуникационных систем стандартов LTE и LTE-Advanced. Данный инструмент ускоряет разработку LTE-алгоритмов и физического уровня (PHY), предоставляет эталонный образец для проверки и тестирования на соответ- ствие стандарту, а также позволяет генерировать тестовые сигналы. С помощью LTE System Toolbox можно производить настройку, моделирование, измерения и анализ канала связи. Также можно создавать и повторно использовать сценарии тестов для подтверждения того, что проекты, прототипы и разработки соответствуют стандарту LTE.

Основные особенности:

• Модели, соответствующие стандартам LTE и LTE-Advanced (Release 8, 9, 10 и 11). • Функции обработки на канальном уровне, поддержка от 1 до 10 режимов передачи по нисходящему каналу, образцы проектов, в том числе CoMP.

• Тестовые модели (E-TM), эталонный измерительный канал (RMC) для LTE, LTE-A, а также генератор UMTS-сигналов.

• Интерактивные инструменты для проверки на соответствие стандарту и BER тестов.

• Передача и приём сигналов при помощи радиоустройств для тестирования систем в реаль- ном эфире.

• Выделение системных и контрольных параметров из принятого сигнала, в том числе cell ID, MIB и SIB1. • Оценка канала связи.

Сквозное моделирование LTE

System Toolbox даёт возможность моделировать и имитировать физический уровень стандарта LTE. Моделирование системы на канальном уровне позволяет добиться требуемых значений характеристик системы, в том числе пропускной способности и BER, а также опреде- лить конкретные реализации системы на основе производимых измерений.

LTE System Toolbox также позволяет улучшить планирование системы, облегчая моделирование канального уровня, которое предоставляет некоторые параметры, необходимые для проектирования базовых станций с заданной геометрией и характеристиками распространения сигнала.

Набор поддерживаемых функций для моделирования режимов передачи и приёма, а также канала связи, включает в себя:

• режимы FDD и TDD на несущих частотах; • все полосы передачи LTE-сигналов от 1,4 до 20 МГц, LTE-A до 100 МГц с агрегацией несущей; • различные типы LTE-сигналов, включая нисходящие и восходящие опорные сигналы и сигналы синхронизации;

• физические LTE-каналы, в том числе каналы управления и каналы общего доступа; • готовую процедуру обработки нисходящего канала, в том числе формирование нисходящего общего канала и канала управления, все возможные MIMO-режимы и генерацию OFDM-сигналов;

• готовую процедуру обработки восходящего канала, в том числе формирование восходящих общего канала и канала управления, SU-MIMO и MU-MIMO режимы и генерацию SC-FDMA сигналов;

• адаптацию к каналу связи, включая схемы выбора типов модуляции и кодирования (MCS) в соответствии с оценкой качества канала связи (CQI), индикатора ранга (RI) и индикации матрицы прекодера (PMI);

• возможности и примеры построения LTE-Advanced, в том числе приём и передача с несколькими eNB (CoMP) и с агрегацией несущей;

• модели распространения LTE-сигналов, в том числе модель пешехода (EPA), модель автомобиля (EVA), модель типичный городской застройки (ETU), модель распространения в движении, а также модели MIMO-каналов в скоростном поезде. LTE System Toolbox даёт возможность создавать тесты, измеряющие пропускную способность PDSCH-канала в соответствии с указанными в стандарте LTE (TS 36.101) условиями испытаний. Структуры данных в LTE System Toolbox позволяют удобно отображать все параметры системы. Функции данного инструмента отражают любые возможные комбинации режимов работы передатчиков, моделей каналов и приемников. Используя этот инструмент для тестирования на соответствие стандарту и BLER-тестирования, вы можете измерять характеристики системы и сравнивать их с указанными в спецификации к стандарту

На рисунке 10.12 изображена структурная схема программного комплекса.

Рис. 10.12. Структурная схема программного комплекса

Для генерации тестового сигнала от базовой станции к абоненту используется генератор LTE-Downlink E-TM Generator.

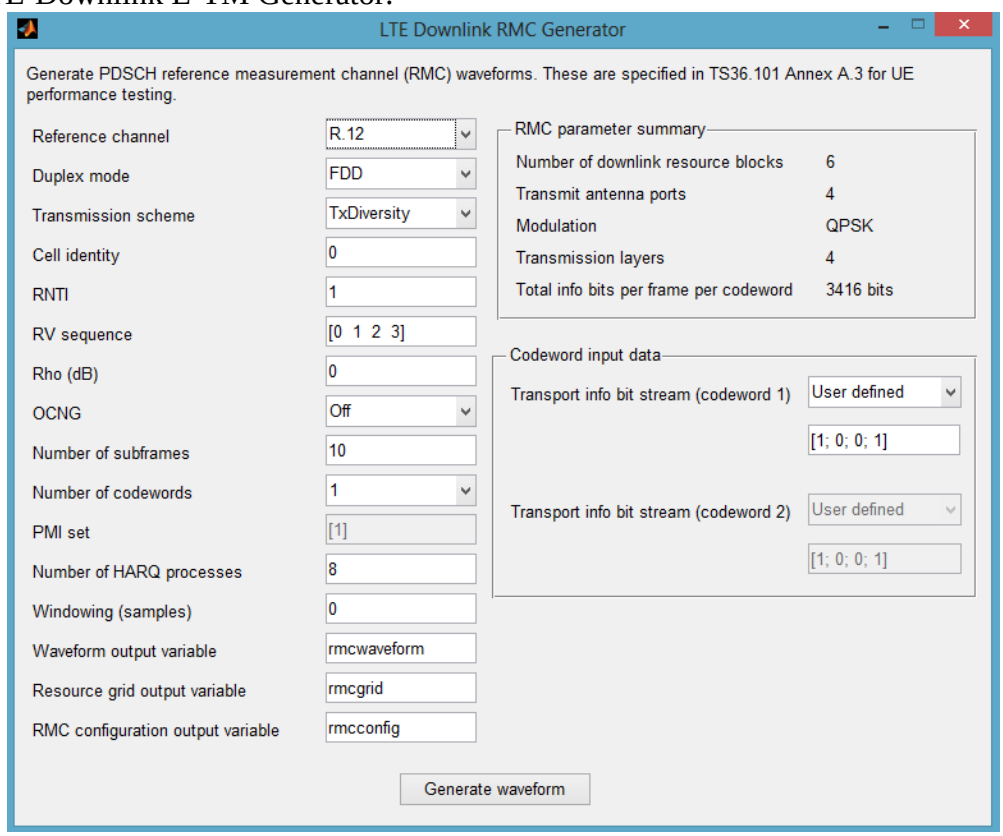


Рис. 10.13. Окно генератора от базовой станции к абоненту

В данном окне задаются параметры генерируемого сигнала на базовой станции, такие как: Количество каналов, вид модуляции, количество обслуживаемых абонентов в секунду, число кодовых слов, вектор инициализации.

На рисунке 19.14 показан вид сгенерированного сигнала, а на рисунке 10.15 трех мерный спектр полученного сигнала.

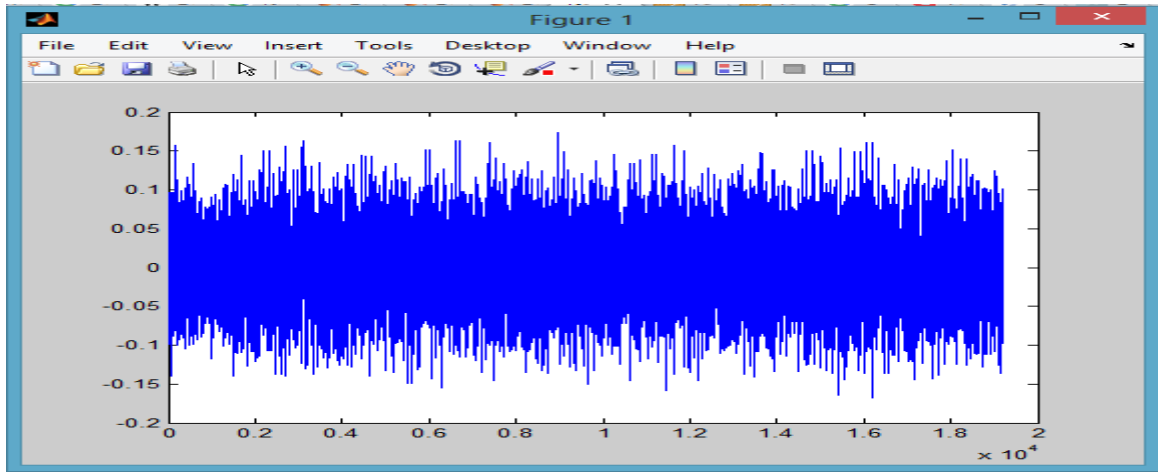


Рисунок 10.14. Сгенерированный сигнал станцией

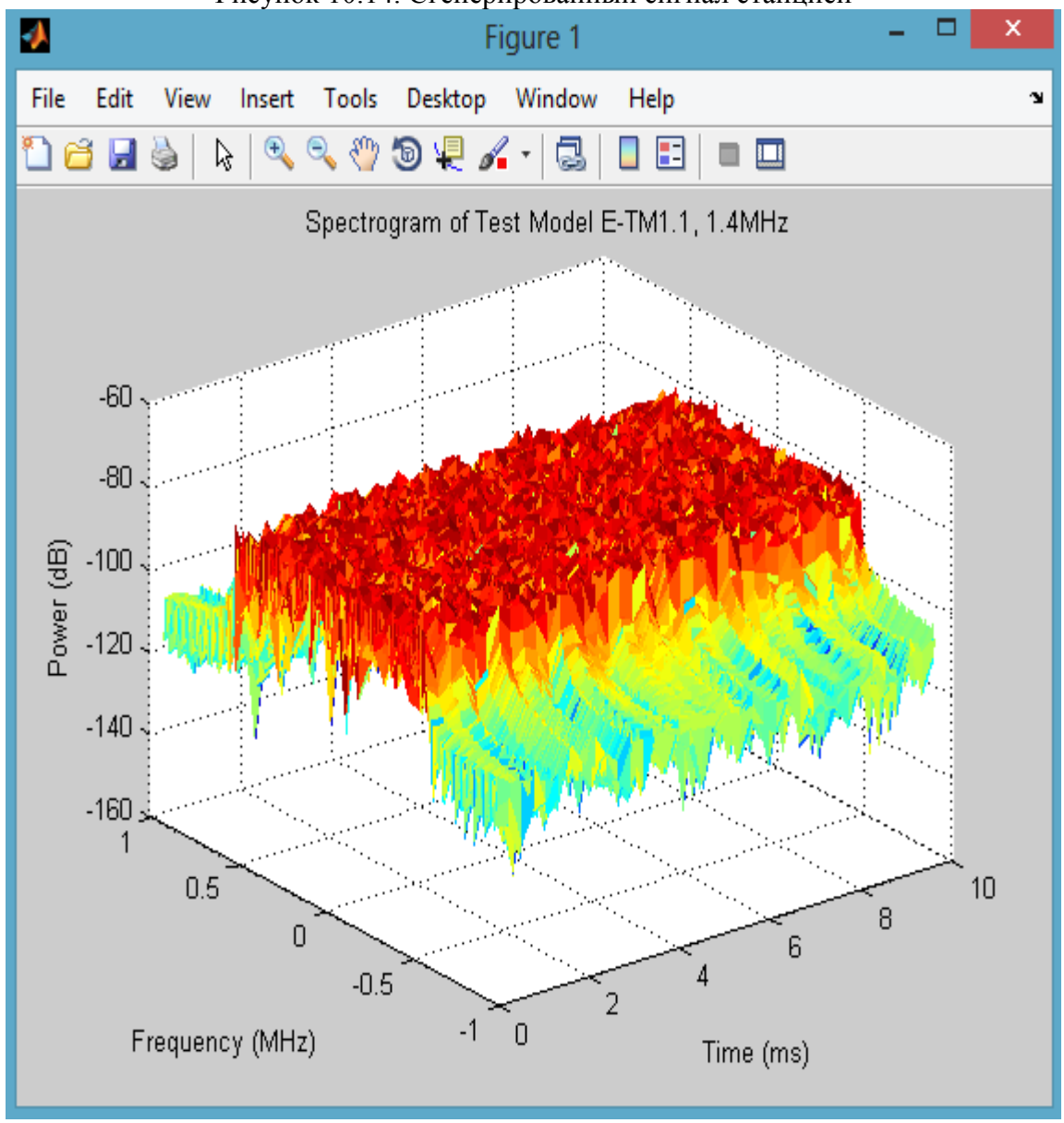


Рис. 10.15. Спектр сгенерированного сигнала станцией в течении 10 секунд

Для генерации тестового сигнала от абонента к базовой станции используется генератор LTE-Uplink RMS Generator.

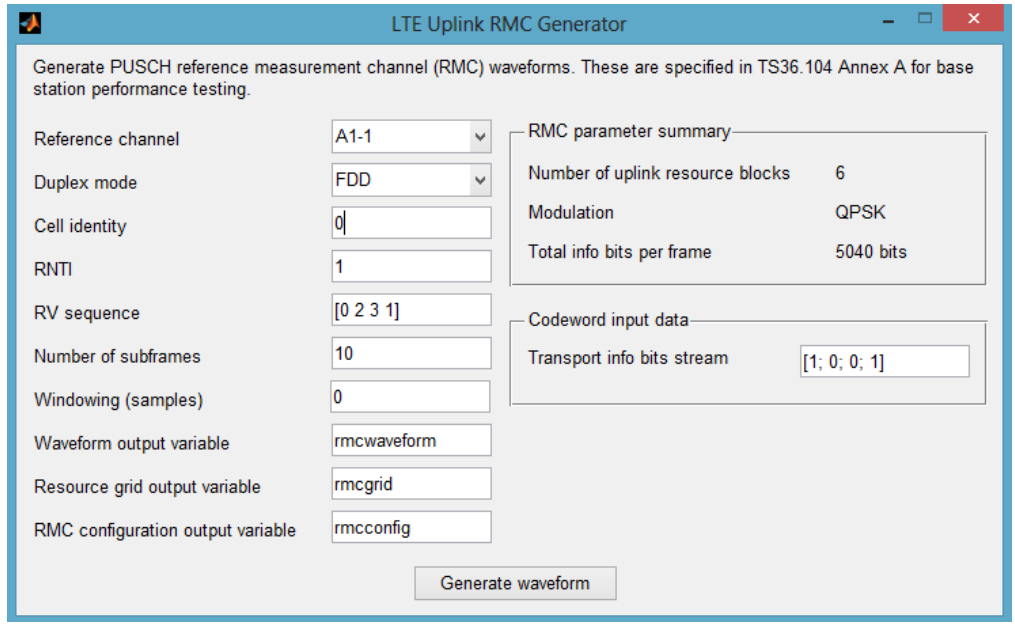


Рис. 10.16. Окно генератора LTE-Uplink RMS Generator

В окне на рисунке 10.16 производятся настройки параметров генерирования от абонента к базовой станции, такие как: Количество каналов для передачи потока пакетов, тип модуляции, вектор инициализации, количество передаваемых пакетов в секунду.

Сигнал, генерируемый генератором LTE-Uplink RMS Generator, представлен на рисунке 10.17.

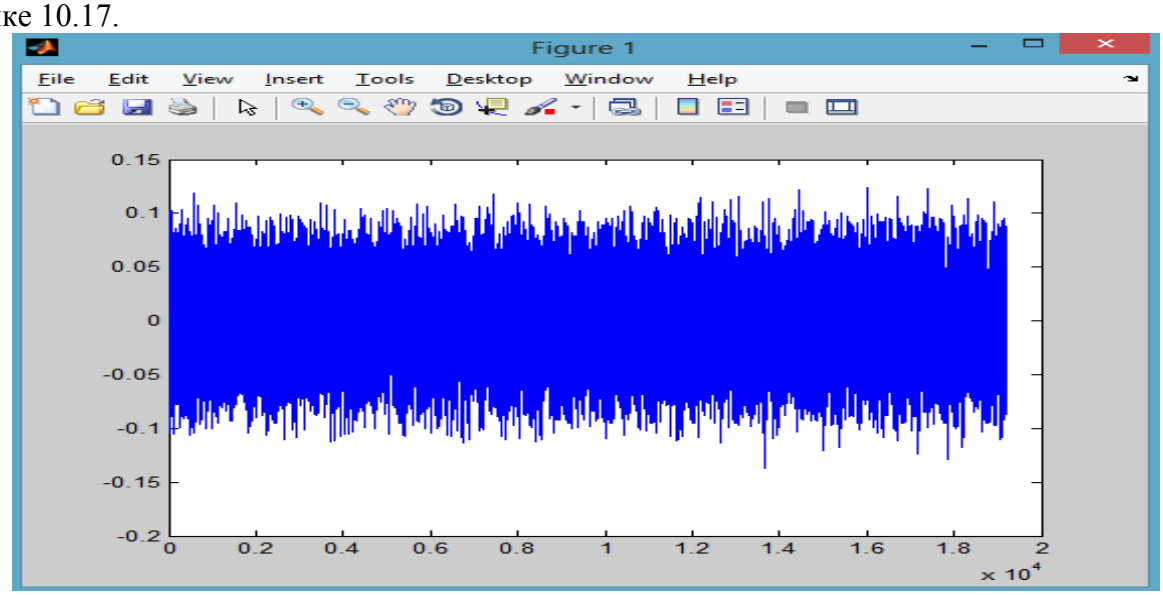


Рис. 10.17. Сигнал генерируемый генератором LTE-Uplink RMS Generator

Для вычисления потерь и пропускной способности системы передачи можно использовать блок LTE PDSCH Conformance Testing.

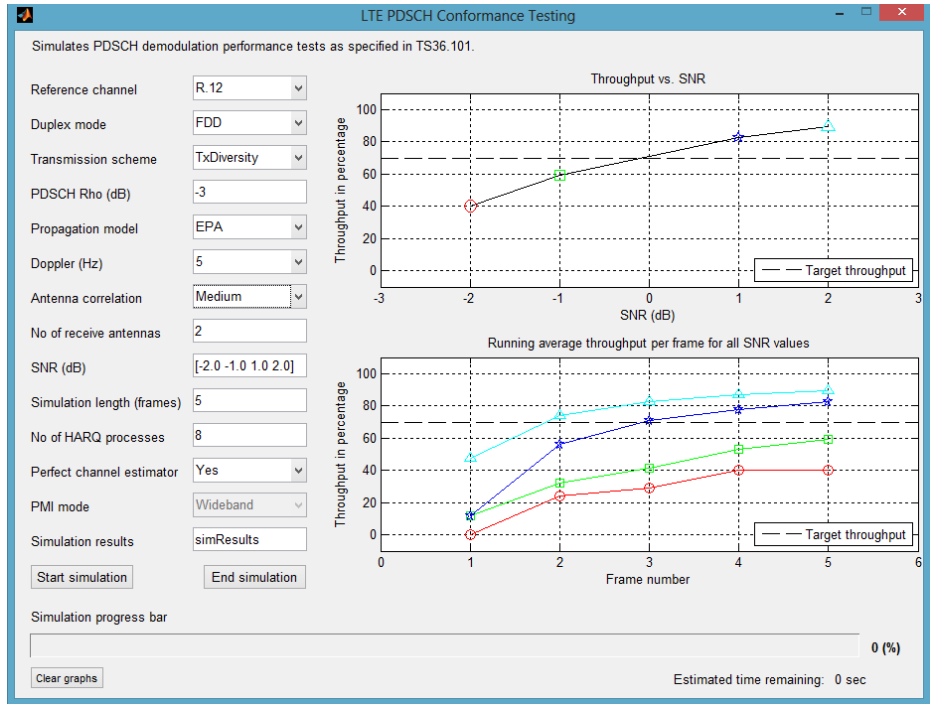


Рис. 10.18. Окно LTE PDSCH Conformance Testing

В данном окне можно произвести настройку параметров линии передачи, таких как: количество каналов, тип модуляции, доплеровскую частоту, уровень шума, настройки антенны и другие. А так же наглядно пронаблюдать изменение количества потерь в линии передачи и пропускную способность системы.

В результате проделанной работы были изучены основные понятия беспроводных сетей LTE, физическая структура построения беспроводной сети LTE. Изучена существующие методы и средства защиты беспроводных сетей LTE. Построена программная структурная схема беспроводной сети LTE среде Matlab с использование встроенного пакета LTE System Toolbox и проведены исследования основных узлов сети LTE.

11. Задание на самостоятельную работу

Криптоанализ шифров гаммирования

Целью работы является получение практических навыков криптоанализа аддитивных двоичных шифров методом вероятных слов. Для того, чтобы не загромождать основную цель рутинными действиями в данной работе были сделаны некоторые упрощения по сравнению с реальными ситуациями. Такими упрощениями являются:

- Заранее известная длина регистра
- Короткое сообщение
- Выбор только из наиболее вероятных биграмм (8 штук)

Задание на лабораторную работу

Заданием для данной лабораторной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. **После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси** и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

Общее описание лабораторной работы

Целью работы является приобретение практических навыков криптоанализа аддитивных шифров.

Результатом работы является получение осмысленного открытого текста из зашифрованного сообщения при помощи учебной программы, называемой «Криптоанализ аддитивного шифра LSR». Лабораторная работа представляет собой исполняемый файл LSR.exe (учебная программа) и набор из 25 вариантов задания (зашифрованный текст).

Общий вид окна учебной программы

Программа LSR.exe представляет собой исполняемый файл, который запускается двойным нажатием на пиктограмму

Рис 1.22. Пиктограмма LSR

После чего на экране появляется диалоговое окно, представляющее собой окно лабораторной работы (рабочее окно).

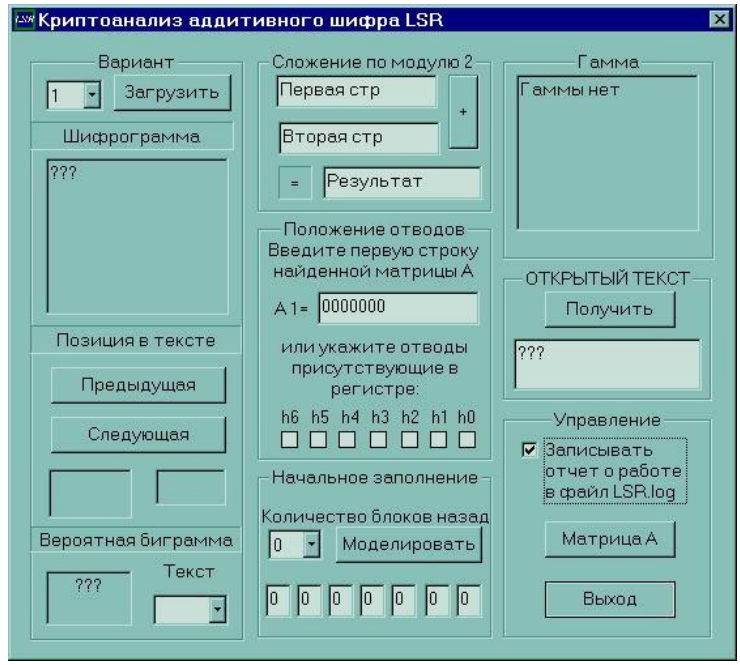


Рис 1.23. Внешний вид окна LSR

Рабочее окно лабораторной работы разделено на 7 блоков, которые представляют собой отдельно последовательно выполняемые шаги лабораторной работы и блок управления. Работа последующих блоков базируется на результатах работы предыдущих.

Кратко перечислим и поясним эти блоки:

- Вариант. Блок предназначен для загрузки внешнего файла варианта в соответствии с выбранным номером, отображения текста задания (подзаголовок Шифрограмма) в зашифрованном виде в битовом представлении и выбора одной из наиболее вероятных биграмм (подзаголовок Вероятная биграмма). Кроме того в блоке находятся кнопки управления «Предыдущая» и «Следующая» для перехода к соответственно предыдущий и последующей позиции, которая является вероятной позицией для биграммы;
- Сложение по модулю два. Блок предназначен для отыскания части вероятной гаммы путем сложения по модулю два битового представления вероятной биграммы и битового представления выбранной части зашифрованного текста;
- Положение отводов. Блок предназначен для ввода строки матрицы А, которая определяет положение отводов в регистре, или указания положения отводов путем заполнения соответствующих полей. **Положение отводов определяется студентом используя подпрограмму**, которая вызывается нажатием кнопки «Матрица А». **Выполняющий составляет вектора S(1),…,S(8)** и подпрограмма, используя метод основанный на нахождении обратной матрицы (с помощью метода Гаусса), находит матрицу обратную к X1 и матрицу А (значение первой строки, которой необходимо для определения положения отводов).
- Начальное заполнение. Блок предназначен для поиска начального заполнения выбранного регистра в соответствии с частью вероятной гаммы. Блок позволяет моделировать работу регистра на некоторое число блоков назад (1 блок=8 шагов) и получать таким образом нужное начальное заполнение, которое так же представлено в этом блоке;
- Гамма. Блок предназначен для получения и отображения гаммы, которая получается используя вид регистра и его начальное заполнение;
- Открытый текст. Блок необходим для получения текстового представления открытого текста, который получен сложением шифрованного текста и гаммы по модулю 2 и последующей перекодировкой;

- Управление. Блок является вспомогательным. Он предназначен для управлением автоматическим созданием файла отчета, нахождения матрицы A (имеется кнопка «Матрицап A», вызывающая подпрограмму поиска матрицы A) и для завершения работы (в данном блоке имеется кнопка «Выход», предназначенная для завершения лабораторной работы и закрытия рабочего окна).

Требования к размещению файлов

Для запуска лабораторной работы необходимо наличие файла LSR.exe, для ее выполнения нужен файл соответсвующего варианта (всего 25 различных вариантов $\Rightarrow$ 25 файлов). Файлы вариантов должны располагаться в том же каталоге, что и LSR.exe. Заметим, что файл отчета lsr.log будет создаваться так же в том же каталоге.

Необходимые знания

Для успешного выполнения лабораторной работы требуются базовые знания в области аддитивных шифров, в частности общие понятия о принципе действия линейного сдвигового регистра, а также пользовательские навыки работы с ОС Windows. Изложенный ранее краткий теоретический материал является достаточным для выполнения лабораторной работы.

Загрузка варианта

Каждому студенту преподавателем назначается вариант, и в соответствии со своим вариантом студент выполняет лабораторную работу.

Для загрузки соответствующего варианта предназначено поле выбора и кнопка «Загрузить» в верхней части блока «Вариант»

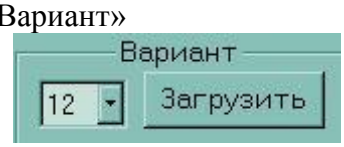


Рис 1.24.Часть блока вариант

Выполняющий работу (студент) выбирает один из предложеных 25 номеров варианта и нажимает кнопку «Загрузить»

Рис 1.25. Кнопка «Загрузить»

После нажатия кнопки в поле для чтения «Шифрограмма» появляется зашифрованный текст в битовом представлении или возникает сообщение об ошибке (см. Сообщения выдаваемые в процессе работы). Задачей выполняющего является расшифровка данного текста.

Рис 1.26. Поле для чтения «Шифрограмма»

В поле для чтения «Шифрограмма» располагается двоичное представление зашифрованного текста. Каждые восемь бит в совокупности представляют собой одну закодированную букву. Ознакомиться с кодировкой можно в Приложении 1.

Всего в поле для чтения «Шифрограмма» представлено 16 закодированных букв (128 бит), таким образом зашифрованный текст представляет собой слово или фразу из 16 символов.

Выбор вероятных составляющих

Поскольку для дальнейшего расшифрования текста (а именно отыскания начального заполнения еще неопределенного регистра) нам требуется 2*L бит гаммы (L – разрядность регистра, в работе n=7 ⇒ требуется 14 бит), то следующим шагом в выполнении работы является определение вероятной биграммы и ее положения в зашифрованном тексте. Для этого предназначено поле выбора «Вероятная биграмма»

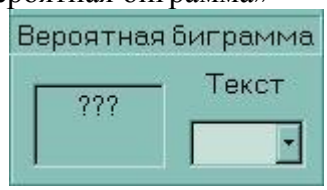


Рис 1.27. Поле «Вероятна биграмма»

На выбор выполняющему работу предлагается 8 биграмм (ЕН, ЕТ, НА, НИ, ПР, РА, СТ, ТО). Эти биграммы являются наиболее вероятными в русском языке, следовательно хотябы одна из них должна содержатся в зашифрованном сообщении (см. полную таблицу вероятностей биграмм в тексте в Приложении 2).

После выбора в поле «Текст» выроятной биграммы в соседнем поле для чтения появится битовое представление этой биграммы, кроме того тоже битовое представление появится в поле ввода «Вторая стр» блока «Сложение по модулю 2».

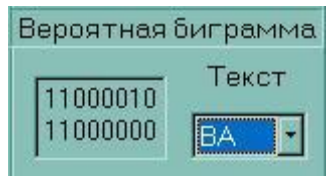


Рис 1.28. Выбранная биграмма

На этом выбор вероятной биграммы закончен. Теперь необходимо определить ее положение в тексте. Будем последовательно перебирать все возможные положения данной биграммы при помощи двух управляющих кнопок «Предыдущая» и «Следующая» (подзаголовок Позиция в тексте).

Рис 1.29. Позиция в тексте и управляющие кнопки

При нажатии на кнопку «Следующая» или «Предыдущая» в левом поле рис 7 появится часть шифрограммы, которая соответствует позициям, номера которых появятся в правом поле для чтения. Одновременно с этим поизойдет заполнение первого поля в блоке «Сложение по модулю 2» содержимым левого поля.

После того как выбрана биграмма и ее положение (то есть заполнены два верхних поля в блоке «Сложение по модулю 2»), в поле «=» блока «Сложение по модулю 2» появится результат сложения.

На этом определение вероятного местоположения вероятной биграммы и части вероятной гаммы закончен. Таким образом мы имеем предполагаемую биграмму, ее предполагаемое местоположение и, вероятно, часть ключа. Дальнейшие шаги покажут нам правильность или ошибочность выбора предполагаемых компонентов.

Нахождение вероятной части ключа

Данный шаг необходим для ручного сложения по модулю 2 собственных компонентов, то есть на предыдущем шаге вероятная часть ключа была найдена автоматически. Таким образом данное описание можно пропустить.

Для определения вероятной части ключа мы будем использовать блок «Сложение по модулю 2» с внесенными в него на предыдущем шаге начальными данными (вероятной биграммой и соответствующей ей части зашифрованного текста).

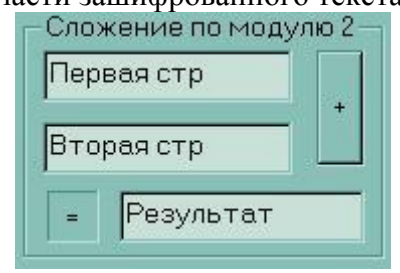


Рис 1.30. Блок «Сложение по модулю 2»

Поскольку для определения вероятной части гаммы достаточно простого сложения по модулю два вероятной биграммы и соответствующей ей части зашифрованного текста, то для получения необходимо нажать кнопку «+».

Рис 1.31. Кнопка «+» (сложить)

После чего в поле «=» появится искомая часть вероятной гаммы.

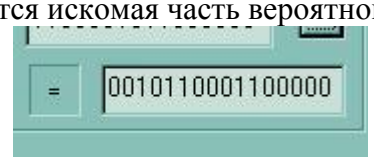


Рис 1.32. Поле «=» - результат сложения

Таким образом мы определили 16 бит ключевой последовательности, которые нужны нам для отыскания положения отводов в регистре, начального заполнения регистра и, как следствие, всей гаммы и открытого текста. Строго говоря, 2 бита из этой последовательности являются избыточными, поскольку для определения положения отводов нужно 2*7=14 бит, а для получения начального заполнения всего 7 бит, но в связи с выбранной кодировкой символов приходится учитывать и эти 2 бита.

Определение положения отводов

Одним из ключевых шагов в выполнении работы является нахождение положения отводов в регистре. В данной работе предполагается определение положения отводов при помощи метода основанного на нахождении обратной матрицы методом Гаусса, используя подпрограмму для обращения матрицы и нахождения матрицы А.

Для определения положения отводов выполняющему необходимо вызвать подпрограмму нахождения матрицы А, нажатием кнопки «Матрица А».

Рис 1.33. Кнопка «Матрица А»

Затем в появившемся диалоговом окне необходимо заполнить поля представляющие собой поля для ввода векторов-столбцов S(1)…S(8) (см. Теоретическое введение).

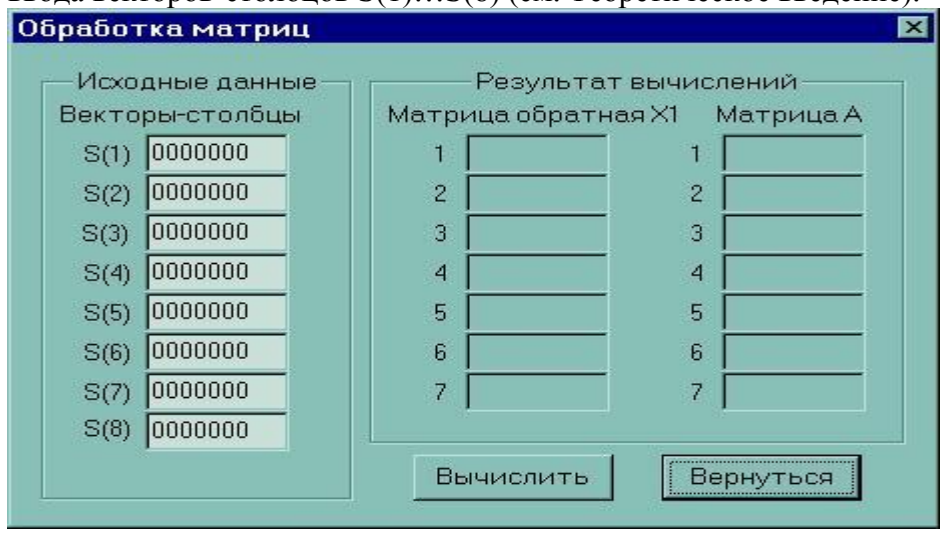


Рис 1.34. Окно подпрограммы для нахождения матрицы A

После корректного заполнения вышеуказанных полей, необходимо нажать кнопку «Вычислить» и в соответствующих полях окна подпрограммы появятся строки соттветствующие матрицам X^{-1} и A.

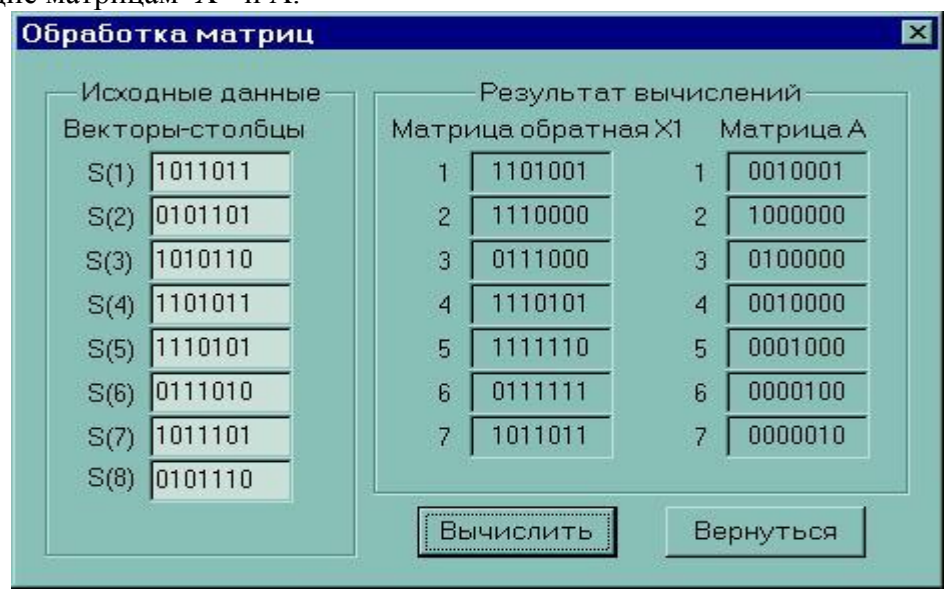


Рис 1.35. Результат работы после нажатия на кнопку «Вычислить»

Следует отметить, что матрица A должна иметь специальный вид: первая строка – определяет положение отводов, в остальных строках под главной диаганалью находятся единицы, остальные нули. Если найденная матрица отличается по виду от вышеописанной, то была допущена ошибка на ранних шагах (например выбрана ошибочная биграмма). Строка 1 подраздела «Матрица A» является определяющей, то есть именно ее вид определяет положение отводов и именно ее необходимо заносить в поле A1 блока положение отводов, после выхода из подпрограммы (нажатием кнопки «Вернуться»).

Рис 1.36. Блок положение отводов

Поскольку для определение отводов существует, по крайней мере, два способа определения положения отводов, то возможно 2 способа заполнения положения отводов. Рассмотрим эти способы.

1) Если отводы были определены при помощи нахождения обратной матрицы, то удобно ввести в поле «А1=» первую строку матрицы А, что будет являться заданием положения отводов и будет продублировано в нижней части блока.

Регистр по условию лабораторной работы является 7-разрядным, то есть первая строка матрицы А является последовательностью из 7 бит, каждый из которых говорит о наличии (если бит равен 1) или отсутствии (если бит равен 0) отвода в регистре.

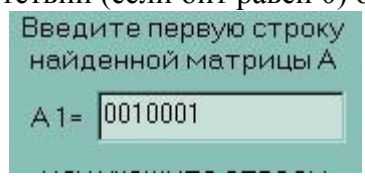


Рис 1.37. Строковое задание положения отводов

Если положение отводов были найдены другим способом, то удобно непосредственно указать отводы присутствующие в регистре, то есть активировать чек-бокс соответствующий присутствующему отводу, введенные данные продублируются в строке «А1=»

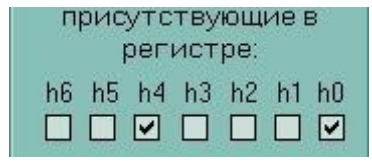


Рис 1.38. Непосредственный выбор отводов

Необходимо внимательнее подходить к проблеме поиска отводов в регистре, так как неправильное определение положения отводов влечет за собой неправильный результат.

Поиск начального заполнения

Для того, чтобы расшифровать текст необходима гамма такой же длины как и зашифрованный текст. Для получения гаммы нам нужно знать начальное заполнение регистра. Для определения начального заполнения в лабораторной работе используется блок «Начальное заполнение».

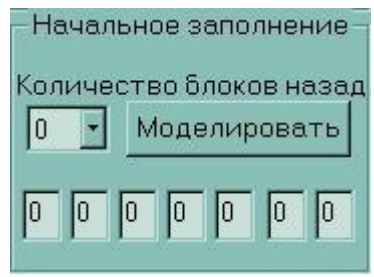


Рис 1.39. Блок «Начальное заполнение»

Поскольку для получения начального заполнения необходимо промоделировать обратную работу регистра, то существует кнопка «Моделировать», при нажатии на которую происходит обратное моделирование работы регистра на заданное количество шагов, которое задается в поле выбора «Количество блоков назад».

Рис 1.40. Кнопка «Моделировать»

Поскольку нецелесообразно моделировать обратную работу на число шагов не кратное 8 (так как 1 символ закодирован 8 битами), то число шагов заменено числом блоков. То есть 1 блок = 8 шагов, и при моделировании на 1 блок производится обратная работа на 8 шагов. Выбор количества блоков назад ограничен 14 (для обеспечния отсутствия цикличности).

Выбор количества блоков на которое производится обратное моделирование важен для правильности определения начального заполнения. Количество блоков для обратного моделирования является первой цифрой в номере позиции вероятной биграммы (см. Подзаголовок «Позиция в тексте» блока «Вариант» правое поле для чтения). То есть если позиция представлена как 3-4 (то есть вероятная биграмма находится на позиции 3 и позиции 4), то обратное моделирование должно производиться на 3 блока назад.

После нажатия на кнопку «Моделировать» автоматически производится поиск начального заполнения регистра. Для этого используются первые 7 бит строки «=» блока «Сложение по модулю 2» и регистр из блока «Положение отводов» (точнее положение его отводов). Полученный результат отображается в схематичном представлении ячеек регистра, заполненных нулями или единицами.

Рис 1.41. Схематичное представление ячеек регистра

Кроме того для удобства выполнения работы сразу после нажатия кнопки «Моделировать», если не произошло никаких ошибок заполняются поля в блоках «Гамма» и «Открытый текст». Таким образом после нажатия кнопки «Моделировать» **при правильном выборе вероятной биграммы, ее положения в тексте и правильного определения положения отводов получается открытый текст.**

Получение гаммы

Для расшифрования сообщения нам необходимо получить гамму, которая использовалась при зашифровке. Этот шаг выполняется автоматически при нажатии на кнопку «Моделировать» из блока «Начальное заполнение». Для контроля за правильностью гаммы предназначен блок «Гамма»

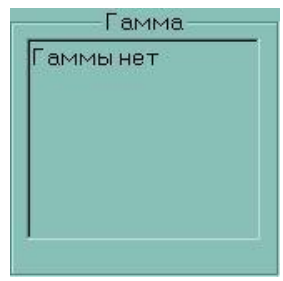


Рис 1.42. Блок «Гамма»

Гамма представляет собой последовательность 128 двоичных символов, которые выводятся в поле для чтения «Гамма». Данная последовательность используется для последующего сложения по модулю 2 с шифрограммой и получения открытого текста в битовом представлении.

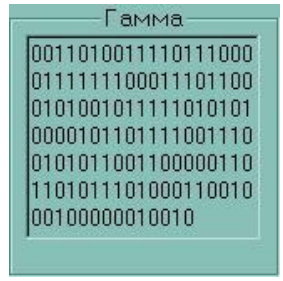


Рис 1.43. Поле для чтения «Гамма»

Получение открытого текста

Открытый текст получается автоматически при нажатии на кнопку «Моделировать» блока «Начальное заполнение», однако для контроля предусмотрены дополнительный возможности.

Открытый текст представляется в программе перекодированным из битовой последовательности в символы и для этого используется блок «ОТКРЫТЫЙ ТЕКСТ».

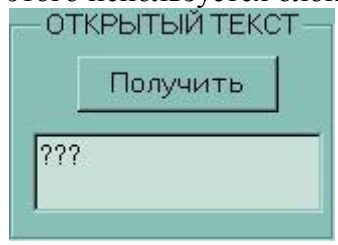


Рис 1.44. Блок «Открытый текст»

Для получения открытого текста достаточно нажать кнопку «Получить». Программа автоматически произведет сложение гаммы и зашифрованного текста, а потом перекодирует битовый текст в символьный.

Рис 1.45. Кнопка «Получить»

В результате в поле ввода появится некоторый текст, который либо представляет собой осмысленное сообщение (тогда работа успешно завершена), либо непонятный набор символов (увы, придется повторить некоторые шаги заново). Во втором случае наиболее вероятным местом ошибки является неправильно выбранное количество блоков для обратного моделирования (как следствие неправильные начальное заполнения и гамма). Если же вы уверены в своих действиях по выбору количества блоков, тогда неверно выбрана биграмма или ее положение (то есть придется вернуться к п 5.3.4), кроме того возможно неверное определение положения отводов (придется вернуться к п 5.3.5)

Если полученный открытый текст устраивает выполняющего то работа завершена.

Отчет о проделанной работе

Для контроля за выполнением работы предусмотрено специальное средство – отчет о проделанной работе. В данной лабораторной отчет представляется в форме файла отчета:

- файл отчета – необходим для предоставления проверяющему (преподавателю);

Форма отчета включаются путем выбора соответствующего элемента в блоке «Управление».

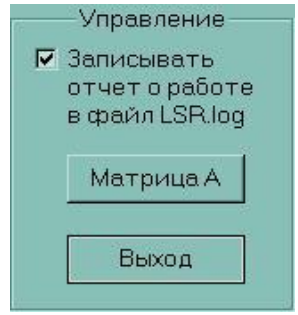


Рис 1.46. Блок «Управление»

Выключатель «Записывать отчет о работе в файл LSR.log» включает\выключает режим записи произведенных действий в файл «lsr.log».

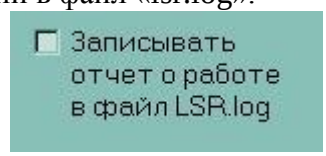


Рис 1.47. Выключатель «Записывать отчет о работе в файл LSR.log»

При включении данного выключателя создается или перезаписываетя или дозаписывается (в зависимости от ситуации) файл «lsr.log», в который записываются действия пользователя по отысканию открытого текста.

Для составления отчета надо:

a) После запуска лабораторной работы включить переключатель «Записывать отчет о работе в файл LSR.log» (включен по умолчанию). Если уже существует lsr.log, то ответить на вопрос: «Переписывать?». Если такого файла нет, то он создастся;

b) Загрузить вариант. В файле появится запись «Начало LOG*********»;

c) Выполнить действия по поиску открытого текста;

d) Найти открытый текст.

e) Выйти из программы при помощи кнопки «Выход». В файле появится запись «Конец LOG*********».

Рис 1.48. Кнопка «Выход»

В файле отчета будут задокументированны основные действия по поиску открытого текста. Отчет предоставляется в распечатанном виде от фразы «Начало LOG**********» до фразы «Конец LOG**********».

ЗАКЛЮЧЕНИЕ

Защита информации представляет в настоящее время одно из ведущих направлений обеспечения безопасности государства, организации, отдельного человека. Проблемы различных аспектов безопасности все более занимают умы специалистов, так как на собственном опыте люди приходят к выводу, что нельзя обеспечить эффективную деятельность государства и организации, а также достойное «качество» жизни человека, отбиваясь от угроз, как от комаров в болотистом месте - усилий много, а толку мало.

Путь решения проблемы безопасности, как и других проблем, начинается с системного подхода к ней и ее системного анализа.

В практике системного анализа укоренилось мнение, что 50% успеха в решении сложной задачи - ее правильная постановка.

Чем более четко определены источники защищаемой информации, места и условия их нахождения, способы и средства добывания информации злоумышленником, тем конкретнее могут быть сформулированы задачи по защите и требования к соответствующим средствам. Конкретность задач и требований - необходимое условие целенаправленного и рационального использования выделенных ресурсов.

Источники информации определяются в результате структурирования защищаемой информации, а места и условия их нахождения - на основе результатов моделирования объектов защиты.

Рост числа и видов угроз безопасности информации, сопровождающих повышение значимости информации в жизни общества и человека, представляют собой тенденцию, которую нельзя не учитывать.

Примером этого могут служить последствия широкого внедрения средств подвижной телефонной связи. Наряду с большими преимуществами для пользователей этого сравнительно нового для России вида связи по сравнению с традиционной проводной телефонной связью, возникла очень серьезная проблема по обеспечению конфиденциальности разговора. Если для несанкционированного подслушивания телефонного разговора в проводном канале злоумышленнику надо предпринять ряд довольно сложных и уголовно наказуемых по закону действий, то для подслушивания разговора по сотовой связи достаточно иметь небольшую сумму денег для покупки сканирующего приемника. С помощью такого приемника можно в комфортабельных условиях и безопасно прослушивать и записывать разговоры абонентов этой системы связи.

Поэтому изучение угроз, знание их потенциальных возможностей применительно к конкретным условиям, умение оценивать угрозы количественной мерой и, наконец, формулирование требований к способам и средствам защиты - необходимые и последовательно реализуемые процессы этапа постановки задач по защите информации. Игнорирование этих процессов может привести к несоответствию применяемых способов и средств защиты информации ее угрозам и, как следствие, - к большим затратам от хищения информации и неоправданными расходами на ее защиту.

Сложность выявления и анализа рассмотренных в книге угроз безопасности информации обусловлена многообразием способов и средств добывания информации, высокой динамичностью их изменения и многовариантностью действий злоумышленников.

Вследствие этого необходимым условием для грамотной постановки задачи по защите информации является постоянное слежение специалистов за состоянием развития соответствующих областей науки и техники, а также моделирование угроз конкретной защищаемой информации. Чем точнее и полнее учтены в требованиях потенциальные угрозы, тем выше можно обеспечить эффективность защиты информации. Грубые ошибки при анализе угроз нельзя исправить на последующих этапах.

Не менее ответственные и сложные задачи возникают при непосредственном выборе рациональных способов и средств защиты, т. е. таких, которые обеспечивают требуемый уровень защиты при минимальных затратах, не превышающих ущерб от хищения информации. В нахождении рациональных вариантов, удовлетворяющих этим условиям, состоит основная проблема этапа определения способов и средств зашиты информации. Несмотря на многообразие возможных способов инженерно-технической защиты, их методы можно свести к двум группам: информационному и энергетическому скрытию информации. Независимо от вида и носителя информации информационное скрытие сводится к маскировке и дезинформированию, а энергетическое - к уменьшению энергии носителя или повышению уровня помех на входе приемника злоумышленника. Такой общий подход к защите информации позволяет рассматривать с единых позиций все многообразие способов и реализующих их средств обеспечения безопасности информации и создает основу для преобразования набора эмпирических рекомендаций по инженерно-технической защите информации в соответствующую теорию.

Основными направлениями дальнейшего развития инженерно-технической защиты информации являются:

- в теоретическом плане - разработка теории инженерно-технической защиты информации как составляющей теории информационной безопасности;
- в методологическом плане - автоматизация процессов рационального решения задач защиты информации в рамках экспертной системы по защите информации;
- в практическом плане - комплексирование способов и средств защиты информации в единую систему защиту для конкретной организационной структуры.

ЛИТЕРАТУРА

Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

Торокин А. А. Основы инженерно-технической защиты информации. М: «Ось-89», 1998. - 365 с.

Хорев А. А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия России, 1998. - 320 с.

Домарев В.В., Безопасность информационных технологий. Системный подход: - К.: 000 «ТИД «ДС», 2004.-992с.

Петраков А.В., Лагутин В.С. Защита абонентского телетрафика. – М.: Радио и связь, 2001. – 504 с.

Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – М.: ООО «Фирма «Издательство АСТ»; СПб.: Издательство «Полигон», 2000. – 272 с.

Энциклопедия промышленного шпионажа./ Ю.Ф.Каторин, Е.В.Куренков, А.В.Лысов, А.Н.Остапенко / Под общей ред. Е.В.Куренкова. – СПб.: ООО «Издательсво «Полигон», 1999. – 512 с.

Технические методы и средства защиты информации/ Ю.Н.Максимов, В.Г.Сонников, В.Г.Петров и др. – СПб.: ООО «Издательсво «Полигон», 2000. – 320 с.

Соколов А.В. Шпионские штучки. Новое и лучшее. – СПб.: ООО «Издательство «Полигон», 2000. – 256 с.

Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Международные отношения, 2000. – 400 с.

Барсуков В.С. Безопасность: технологии, средства, услуги. – М.: КУДИЦ – ОБРАЗ, 2001. – 496 с.

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

Петраков А. В., Дорошенко П. С., Савлуков Н. В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999. - 568 с.

Лагутин В. С., Петраков А. В. Утечка информации в телефонных каналах. М.: Энергоатомиздат, 1996. - 304 с.

Хорев А. А. Методы и средства поиска. Электронные устройства перехвата информации. М.: МО РФ, 1998. - 224 с.

Гавриш В. Практическое пособие по защите коммерческой тайны. Симферополь: "Таврида", 1994. - 112 с.

Петраков А. В. Защита и охрана личности, собственности, информации, Справочное пособие, М.: «Радио и связь», 1997. - 320 с.

Цветков В. В., Демин В. П., Куприянов А. И. Радиоэлектронная борьба: радиоразведка и радиопротиводействие. Учебное пособие. М.: Изд-во МАИ, 1998. - 248 с.

Демин В. П., Куприянов А. И., Сахаров А. В. Радиоэлектронная разведка и радиомаскировка. М.: Изд-во МАИ, 1997. - 156 с.

Волхонский В. В. Устройства охранной сигнализации. СПб.: Экономис и культура, 1999. - 272 с.