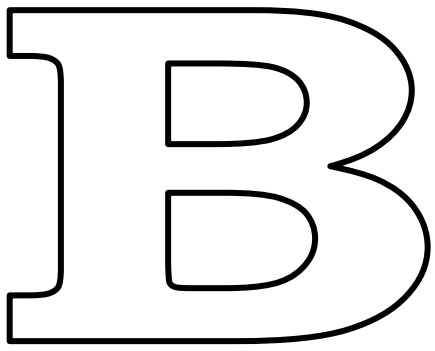


ДЛЯ ВУЗОВ

А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, С.В. Скрыль, И.В. Голубятников

Технические средства и методы защиты информации

Под ред. А.П. Зайцева и А.А. Шелупанова

Рекомендовано Министерством образования и науки РФ в качестве учебника для студентов высших учебных заведений, обучающихся по специальностям
090102 – «Компьютерная безопасность»,
090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем»,
090106 – «Информационная безопасность телекоммуникационных систем»

Москва
«Машиностроение»
2009

ББК 32.81
УДК 681.3.81
Т 38

Рецензент:
доктор физико-математических наук,
профессор *С.С. Бондарчук*

Т 38 Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

ISBN 978-5-94275-454-9

Изложены вопросы теории и практики защиты информации техническими средствами. Значительное внимание уделено физической природе возникновения информационных сигналов в электромагнитных, электрических, акустических и виброакустических каналах утечки информации, методам расчета параметров. Подробно рассмотрены средства выявления технических каналов утечки информации и защита информации от утечки. Отдельный раздел посвящен технически средствам защиты объектов. Приведена классификация основных технических каналов утечки информации, имеющих место в реальных условиях. Рассмотрены вопросы технического контроля эффективности мер защиты информации и аттестации объектов информатизации. Предложены варианты практических заданий. В приложении приводятся технические характеристики некоторых устройств выявления и защиты каналов утечки информации.

Для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности.

ББК 32.81
УДК 681.3.81

ISBN 978-5-94275-454-9

Учебник для вузов

Зайцев Александр Петрович,
Шелупанов Александр Александрович,
Мещеряков Роман Валерьевич,
Скрыль Сергей Васильевич,
Голубятников Игорь Владимирович

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Издается в авторской редакции

000 «Издательство Машиностроение»
107076, Москва, Стромынский пер., 4/1, стр. 3

Редактор Е.М. Малышева
Корректор Н.Г. Генис
Верстка В.М. Бочкаревой

Подписано к печати 15.03.2008.
Формат $60\times84^{1}/_{16}$. Печать офсетная.
Печ. л. 25,75. Усл.печ. л. 24,24.
Тираж 1000 экз. Заказ 67.

Отпечатано в типографии
Московского государственного университета приборостроения и информатики
107996, Москва, ул. Стромынка, 20

Содержание

ВВЕДЕНИЕ

В-1. Виды, источники и носители защищаемой информации

Значение информации в жизни любого цивилизованного общества непрерывно возрастает. С незапамятных времен сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались. В настоящее время информация, относящаяся к технологии производства и сбыта продукции, стала рыночным товаром, имеющим большой спрос как на внутреннем так и на внешнем рынках. Информационные технологии постоянно совершенствуются в направлении их автоматизации и способов защиты информации.

Развитие новых информационных технологий сопровождаются такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации. Поэтому защита информации является важнейшей государственной задачей в любой стране. Острая необходимость в защите информации в России нашла выражение в создании Государственной системы защиты информации (ГСЗИ) и в развитии правовой базы информационной безопасности. Приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных», «Доктрина информационной безопасности Российской Федерации» и др.

Защита информации должна обеспечивать предотвращение ущерба в результате утери (хищения, утраты, искажения, подделки) информации в любом ее виде. Организация мер защиты информации должна проводиться в полном соответствии с действующими законами и нормативными документами по безопасности информации, интересами пользователей информации. Чтобы гарантировать высокую степень защиты информации, необходимо постоянно решать сложные научно-технические задачи разработки и совершенствования средств ее защиты.

Большинство современных предприятий независимо от вида деятельности и форм собственности не может успешно вести хозяйственную и иную деятельность без обеспечения системы защиты своей информации, включающей организационно-нормативные меры и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС).

В законе РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» и в ст. 2 Федерального Закона «Об участии в международном информационном обмене» приводятся следующие определения информации и ее конкретных разновидностей:

− информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

− документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

− информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

− конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

В более общем смысле информация – это сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования для определенных целей. Согласно этому определению человек находится в постоянно изменяющемся информационном поле, влияющем на его образ жизни и действия.

По своему характеру информация может быть политической, военной экономической, научно-технической, производственной или коммерческой и быть секретной, конфиденциальной или несекретной

Согласно законодательному определению конфиденциальная информация должна быть документированной и иметь ограниченный доступ в соответствии с законодательством Российской Федерации. Под такое определение попадает любая защищаемая информация, однако на практике принято защищаемую информацию разделять в зависимости от степени ее конфиденциальности.

По степени конфиденциальности (степени ограничения доступа) в настоящее время можно классифицировать только секретную информацию, составляющую государственную тайну. Согласно статье 8 Закона РФ «О государственной тайне», устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

В соответствии со статьей 2 Закона РФ «О государственной тайне», государственная тайна – вид секретной информации, содержащей защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

К служебной тайне относятся охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства. Служебная тайна относится к секретной информации и имеет гриф «секретно».

К конфиденциальной информации относят сведения, содержащие коммерческую тайну, адвокатскую и следственную тайну, некоторые виды служебной тайны, врачебную тайну, тайну переписки, телефонных переговоров, почтовых и телеграфных отправлений, а также некоторые сведения о частной жизни и деятельности граждан.

Конфиденциальную информацию составляют сведения, порядок доступа к которым определен их собственником в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной только санкционированным лицам, объектам или процессам.

Понятие «коммерческая тайна» определено Законом о предприятиях и предпринимательской деятельности как информация, которая «составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Разглашение коммерческой тайны может серьезным образом повлиять на результаты деятельности предприятия или фирмы, поэтому коммерческая тайна должна быть охраняемой. Руководитель предприятия или организации должен издать приказ, в котором указываются сведения, составляющие коммерческую тайну.

Под определение коммерческой тайны не должны подпадать сведения о видах деятельности фирмы, так как такие сведения могут содержать информацию о влиянии производства на экологию окружающего пространства, о негативных воздействиях на здоровье людей и т.п.

Отличие сведений, составляющих государственную тайну, от коммерческой тайны заключается в том, что они регламентированы соответствующим перечнем и защищаются государством. Коммерческая тайна не имеет перечня, так как она различна для каждого предприятия или фирмы. Ее защиту осуществляют службы безопасности предприятия. Коммерческая тайна может в отдельных случаях относиться и к государственным секретам, если эти секреты имеют важное значение для государства.

Любая тайна представляет собой секрет, но не каждый секрет можно назвать тайной, хотя эти понятия тесно связаны. Коммерческую тайну относят к форме обеспечения безопасности коммерческой информации путем скрытия некоторых сторон деятельности предприятия, а коммерческие секреты содержат документированную информацию или изделия, составляющие секрет фирмы и имеющие важное значение для ее успешной коммерческой деятельности.

Секретность в условиях острой конкурентной борьбы в сфере производства и сбыта продукции призвана защитить производителя в современ-

ных рыночных отношениях от негативных последствий, возможных в результате действий недобросовестных конкурентов. Противоправные действия конкурентов могут выражаться в подделке запатентованной продукции, в незаконном использовании торговой марки производителя, в проведении промышленного шпионажа и т.п.

Несекретная (открытая) информация не относится к государственной, служебной, коммерческой или личной тайне и может быть опубликована в открытой печати. На пользование несекретной информацией не накладывается никаких ограничений. Несекретная информация если представлена в форме документов или банка данных ЭВМ должна защищаться от нарушения целостности и блокирования.

Под термином «тайна» понимают сведения, которые должны быть доступны строго определенному кругу уполномоченных лиц, работающих с этими сведениями и обязанных соблюдать режим неразглашения скрываемых сведений.

В общегосударственном плане тайна означает засекречивание ряда сведений, сокрытие которых от явного или потенциального противника дает государству возможность успешно решать задачи оборонного, политического, научно-технического, информационного и иного характера без значительного ущерба для обеспечения жизнедеятельности страны.

Перечислим некоторые важные типы тайн.

Как уже отмечалось выше, государственные секреты включают в себя государственную и служебную тайны.

Предпринимательские секреты включают в себя промышленную, финансовую и коммерческую тайны.

Коммерческая тайна содержит информацию конфиденциального характера из любой сферы производственной и управленческой деятельности государственного или частного предприятия, разглашение которых может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем на основе государственных законодательных актов. Коммерческая тайна включает в себя также подробности коммерческой деятельности, состав партнеров, источники сырья, технологию сбыта продукции.

Промышленная тайна – это новые технологии, открытия, изобретения, применяемые в процессе производства продукции, и т.д.

Финансовую тайну могут составлять бухгалтерские и финансовые документы, деловая переписка и т.д.

Личная тайна – это сведения конфиденциального характера, разглашение которых может нанести материальный ущерб отдельному (физическому) лицу. Охрана личной тайны осуществляется ее владельцем. Государство не несет ответственность за сохранность личных тайн.

Собственниками (или владельцами) защищаемой информации могут быть органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны); юридические лица (коммерческая, банковская служебная, адвокатская, врачебная, аудиторская тайны и т.п.); общественные организации (партийная тайна, не исключена также государственная и коммерческая тайна); граждане государства (физические лица) – в отношении личной и семейной тайны, нотариальной, адвокатской, врачебной.

Защищаемая информация обладает следующими свойствами:

- уровень доступа к ней, ограничения на порядок распространения и использования может устанавливать только владелец или наделенные таким правом определенные лица;
- чем ценнее для собственника информация, тем тщательнее она защищается и тем меньшее число лиц имеет доступ к этой информации.

Информация по форме представления, способам кодирования и хранения может быть графической, звуковой, текстовой, цифровой (компьютерной), видеоинформацией и т.п.

Наиболее важными свойствами информации являются прежде всего ее достоверность, полнота, объективность, своевременность, важность.

Для хранения как секретной, так и несекретной информации применяются одни и те же носители. В общем случае носители секретной и конфиденциальной информации охраняются ее собственником.

Носители защищаемой информации классифицируются как документы; изделия (предметы); вещества и материалы; электромагнитные, тепловые, радиационные и другие излучения; гидроакустические, сейсмические и другие физические поля, представляющие особые виды материи; сам объект с его видовыми характеристиками и т.п.

В качестве носителя защищаемой информации может быть также человек.

Формы представления информации зависят от ее характера и физических носителей, на которых она представлена. Основными формами информации, подлежащими защите, являются:

- документальные;
- акустические;
- телекоммуникационные;
- видовые.

Документ – представленная на материальном носителе информация с идентификатором, позволяющим установить характер документа и его собственника. Информация, записанная на носителе, может быть графической и текстовой. На документе-носителе защищаемой информации указывается степень конфиденциальности информации в зависимости от ее важности.

Источниками речевой информации являются разговоры в помещениях и системы звукоусиления и звуковоспроизведения. Речевая информация

распространяется в газовой, твердотельной и гидравлической средах. Носителем речевой информации являются акустические колебания частиц в виде звуковых волн различной длины в упругих средах. Слышимый речевой сигнал находится в диапазоне частот 200 Гц – 6 кГц.

Изделия (предметы) как носители защищаемой информации могут представлять собой засекреченные образцы военной техники, опытные образцы вновь разрабатываемых высокотехнологичных изделий и систем, определяющих уровень научно-технического развития промышленности страны.

Материалы и вещества, применяемые в производстве и эксплуатации новых образцов техники и в военных изделиях. Отметим особо, что иностранные разведки могут получать информацию о материалах и веществах наиболее доступными способами – по отходам производства режимных предприятий, по составу воздушной среды и водных осадков в непосредственной близости от предприятия.

Электромагнитные излучения различной частоты могут содержать информативные сигналы от защищаемого объекта при его функционировании. Источником электромагнитного излучения в большинстве случаев являются кабельные и проводные линии каналов передачи информации. Опасными являются также вспомогательные средства и системы, представляющие собой сосредоточенные и распределенные случайные антенны.

Носителем видовой информации объекта является сам объект, а также его фото- и видеоизображения на материальных носителях информации.

С развитием информационного общества все большее значение приобретают проблемы, связанные с защитой конфиденциальной информации. Информация как категория, имеющая стоимость, защищается ее собственником от лиц и организаций, пытающимися ею завладеть. Общая тенденция такова, что чем выше уровень секретности информации, тем выше и уровень ее защиты, тем больше средств затрачивается на ее защиту.

Каждое государство защищает свои информационные ресурсы .

В-2. Классификация иностранной технической разведки. Возможности видов технической разведки

По направлениям разведывательной деятельности иностранные разведки подразделяется на политическую, экономическую, военную и научно-техническую разведки.

Политическая разведка осуществляет деятельность по добыванию сведений внутриполитического и внешнеполитического характера в стране, являющейся объектом разведки, организует действия по подрыву политического строя государства. Примером могут служить организация «цветных революций» в некоторых странах постсоветского пространства, свержение неугодных режимов на Ближнем Востоке.

Экономическая разведка занимается сбором сведений, раскрывающих экономический потенциал определенной страны. К таким сведениям относятся характеристики природных ресурсов, промышленности, транспорта, финансовой системы, торговли и т.п.

Военная разведка направлена на сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники. Особое внимание иностранные разведки уделяют добыванию информации о научно-исследовательских центрах, видных ученых и специалистах.

Научно-техническая разведка занимается добыванием сведений по новейшим теоретическим и практическим разработкам в области науки и техники.

Основные формы разведывательной деятельности:

- агентурная разведка;
- легальная разведка;
- техническая разведка;
- аналитическая обработка первичной информации.

Агентурная разведка использует для добывания информации и проведения диверсионных акций специально подобранных, завербованных и профессионально подготовленных агентов. Агентурная разведка также предполагает добывание информации путем проникновения агента-разведчика к источнику информации на доступное расстояние для применения технических средств разведки.

Легальная разведка добывает информацию при различных официальных связях и контактах с нашей страной, из легальных источников информации.

Существует три основные формы легальной разведки:

- анализ всех открытых публикаций, которые издаются в стране-объекте разведки;
- получение информации во время непосредственных контактов агентов с интересующими их лицами на приемах, встречах, конференциях;
- визуальное наблюдение, кино– и фотосъемка при перемещении иностранцев по стране.

Техническая разведка предполагает сбор информации с использованием технических разведывательных средств.

Аналитическая обработка первичной информации позволяет на основе анализа не систематизированной первичной разведывательной информации с помощью специально разработанных программ обработки получать более объективные разведданные.

Техническую разведку (ТР) можно классифицировать по нескольким признакам. Первый признак связан с используемыми носителями средств добывания информации, в соответствии с которым ТР делится на:

- космическую;
- воздушную;
- морскую;
- наземную.

Второй признак связан с используемой аппаратурой или способами ведения разведки. Согласно этому признаку к ТР относятся следующие виды разведок.

Оптическая и оптоэлектронная разведки, обеспечивающие добывание информации путем приема и анализа электромагнитных излучений ультрафиолетового, видимого и ИК-диапазонов от объектов разведки.

Визуально-оптическая разведка, сущность которой заключается в добывании информации об объектах с помощью оптических наблюдательных приборов или визуально без использования технических средств. Визуально-оптическое наблюдение – наиболее давний способ наблюдения. Современный состав приборов визуально-оптического наблюдения разнообразен – от специальных телескопов, биноклей, монокуляров, зрительных труб до эндоскопов и различных оптических приборов для скрытного наблюдения и регистрации информации в дневных и ночных условиях при любой погоде

Фотографическая разведка, которая предполагает получение видовой информации с помощью специальных фотокамер, установленных на различных носителях. Фотокамеры, установленные на летательных аппаратах, должны иметь высокую разрешающую способность.

Фотосъемка обладает заметными преимуществами перед другими способами разведки, так как позволяет получать оптические изображения объектов с высоким качеством. Изучение фотоснимков дает наибольшее количество разведывательных сведений по сравнению с визуальным, телевизионным или радиолокационным наблюдением, а также при использовании средств инфракрасной разведки. Поэтому специалисты считают фотографирование одним из самых эффективных способов разведки скрываемых объектов.

В зависимости от применяемых фотоматериалов фотографирование в разведывательных целях может быть черно-белым, цветным и спектрозональным. Цветное фотографирование при фоторазведке применяется ограниченно, так как при съемке с больших расстояний цветовые характеристики объекта и фона слаборазличимы, что может привести к ошибочным оценкам полученных результатов.

Спектрозональное фотографирование применяется для получения двухслойного изображения замаскированных объектов путем одновременного фотографирования объектов в двух различных зонах спектра на двухслойную фотопленку. Верхний слой пленки чувствителен только к инфра-

красным лучам, нижний слой – к видимому свету. На фотоснимках объект и фон имеют разный цвет в силу различия отражательной способности в разных зонах спектра и не маскируют друг друга.

На спектрозональных снимках различимы нарушения растительного покрова, дороги, мосты, искусственные объекты, лиственные и хвойные породы деревьев.

Инфракрасная разведка (ИКР) позволяет добывать информацию об объектах при использовании в качестве носителя информации либо собственного теплового излучения объектов, либо отраженного ИК-излучения луны, звездного неба, а также отраженного излучения специальных ИК-прожекторов подсветки объектов. Соответственно этим принципам приборы ИКР делятся на две группы:

1. тепловизионные приборы;
2. приборы ночного видения (ПНВ).

Тепловизионная аппаратура позволяет получать изображение путем регистрации теплового контраста между объектом и окружающим фоном. Достоинствами тепловизионной аппаратуры являются: скрытность ведения разведки ввиду отсутствия подсвечивающих излучений, относительно высокая помехоустойчивость к излучениям в видимой части спектра, способность выявлять замаскированные цели даже в плохих метеорологических условиях (туман, дым, дождь).

Радиоэлектронная разведка (РЭР) позволяет получать информацию путем приема и анализа электромагнитного излучения (ЭМИ) радиодиапазона, создаваемого различными радиоэлектронными средствами.

Радиоэлектронная разведка характеризуется следующими свойствами:

- Проводится без непосредственного контакта с объектами разведки.
- Действует на больших расстояниях в пространстве, пределы которых зависят от частот радиоволн.
- Возможна непрерывность работы при любых условиях.
- Получает достоверную информацию, поскольку ее источником являются радиоизлучающие устройства объекта разведки (за исключением случаев радиодезинформации).
- Получает информацию чаще всего в реальном масштабе времени.
- Обеспечивает в большинстве случаев скрытность. Противник не в состоянии установить факт разведки, если она проводится радиоприемными (неизлучающими) средствами.

Радиоэлектронная разведка подразделяется на виды:

1. Радиоразведка
2. Радиотехническая разведка
3. Радиолокационная разведка
4. Телевизионная разведка

Радиоразведка предназначена для анализа различных видов радиосвязи. Объектами радиоразведки являются средства радиосвязи, радиотелеметрии и радионавигации.

Основное назначение радиоразведки – обнаружение и перехват открытых и кодированных передач связных радиостанций, пеленгование их сигналов, анализ и обработка добываемой информации для определения ее содержания, локализация местоположения источников излучений.

Радиотехническая разведка представляет собой вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (РЛС), радионавигационных и радиотелекодовых систем на основе методов радиоприема, пеленгования и анализа радиосигнала. Объектами радиотехнической разведки могут быть также электромагнитные излучения различных технических устройств.

По результатам радиотехнической разведки можно:

- Установить несущую частоту передающих радиосредств.
- Определить координаты источников излучения.
- Измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры).
- Установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная).
- Определить структуру боковых лепестков излучения радиоволн.
- Измерить поляризацию радиоволн.
- Установить скорость сканирования антенн и метод обзора пространства РЛС.

Радио- и радиотехническая разведки представляют собой пассивные разновидности радиоэлектронной разведки.

Радиолокационная разведка представляет собой активную разновидность РЭР. Применяется для получения видовой информации о местности и объектах на ней. Бывает наземной и воздушной.

Телевизионная разведка предназначена для передачи на расстояние сигналов движущихся или неподвижных изображений по радиоканалу или по проводам. Некоторые системы телевизионной разведки позволяют кодирование передаваемых сигналов. Дальность передачи сигналов телевизионных систем разведки может достигать несколько десятков километров.

Лазерная разведка основана на использовании лазерных сканирующих камер, которые устанавливаются на воздушных носителях и работают в оптическом диапазоне. Поскольку в лазерных системах разведки реализуется строчно-кадровая развертка, то такая система по принципу действия близка к телевизионной. Отраженное фоновой поверхностью и объектами, на ней расположенными, лазерное излучение принимается оптической системой и направляется на чувствительный элемент. Приемник преобразует

отраженное от поверхности излучение в электрический сигнал, который будет промодулирован по амплитуде в зависимости от яркости фрагментов изображения. Изображение регистрируется на фотопленку или может воспроизводиться на экране электронно-лучевой трубки.

Фотометрическая разведка используется для обнаружения и распознавания устройств, в которых используются лазерные источники излучения.

Гидроакустическая разведка обеспечивает съем информации при помощи гидролокатора путем приема и анализа акустических сигналов, распространяющихся в водной среде от различных объектов.

Акустическая разведка обеспечивает получение информации путем приема и анализа акустических сигналов, распространяющихся в различных средах от объектов.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации можно разделить на воздушные, вибрационные, акустоэлектрические, оптико-электронные и параметрические.

• *Воздушные каналы*. В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

• *Вибрационные каналы*. В вибрационных (структурных) каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

• *Акустоэлектрические каналы*. Акустоэлектрические технические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами. Перехват акустических колебаний осуществляется через ВТСС, обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания».

• *Гидроакустический канал* образуется в водной среде и позволяет добывать акустическую информацию с использованием гидрофонов (сонаров).

• *Оптико-электронный канал*. Оптико-электронный (лазерный) канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.

• *Параметрические каналы*. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС. При этом незначительно изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом.

По способу применения технические средства съема акустической информации можно классифицировать следующим образом.

Средства, устанавливаемые заходовыми (требующими проникновения на объект) методами:

- радиозакладки;
- закладки с передачей акустической информации в инфракрасном диапазоне;
- закладки с передачей информации по сети 220 В;
- закладки с передачей акустической информации по телефонной линии;
- диктофоны;
- проводные микрофоны;
- «телефонное ухо».

Средства, устанавливаемые беззаходовыми методами:

- аппаратура, использующая микрофонный эффект;
- высокочастотное навязывание;
- стетоскопы;
- лазерные микрофоны.

Химическая разведка позволяет получить информацию путем анализа изменений химического состава окружающей среды под воздействием выбросов и отходов промышленного производства, взрывов, а также химического заражения местности.

Химическая разведка складывается из непосредственно разведки и химического наблюдения.

Основной задачей химической разведки в мирное время является установление характера химического вещества и его концентрации.

Эта задача решается различными способами с использованием средств индикации (определения) химических веществ. Способы индикации химических веществ могут быть разделены на две группы: субъективные, пли органолептические, основанные на показаниях наших органов чувств, и объективные, основанные на показаниях различных приборов.

Сейсмическая разведка обнаруживает и анализирует деформационные и сдвиговые поля, возникающие в земной коре при различных взрывах.

Магнитометрическая разведка проводится путем обнаружения и анализа локальных изменений магнитного поля Земли, вызванным сосредоточением военной техники, подводными лодками и т.п.

В-3. Основные этапы и процедуры добывания информации технической разведкой

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

– снижение риска физического задержания агента органами контрразведки и службы безопасности за счет дистанционного контакта его с источником информации;

– добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

Основными принципами добывания информации являются следующие:

– целеустремленность;

– активность;

– непрерывность;

– скрытность;

– комплексное использование сил и средств добывания информации.

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

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

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

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

Технология добывания информации предусматривает следующие этапы:

- организацию добывания информации;
- добывание данных и сведений;
- информационную работу.

Организация добывания информации включает:

- декомпозицию (структурирование) задач, поставленных пользователями информации;
- разработку замысла операции по добыванию информации;
- планирование;

- постановку задач исполнителям;
- нормативное и оперативное управление действиями исполнителей и режимами работы технических средств.

Методы доступа к информации можно разделить на три группы:

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

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

Наиболее общим показателем эффективности разведки, включающей органы управления, добывания и обработки, является степень выполнения поставленных перед нею задач. Для более объективного определения эффективности используется группа общесистемных показателей количества и качества информации [39]:

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

Промышленный шпионаж может обеспечить незаконные преимущества над конкурентами, затратившими значительные финансовые и материальные ресурсы на организацию производства своей продукции, имеющей спрос на рынке. Органы коммерческой разведки, входящие в состав службы безопасности, призваны обеспечивать руководство информацией, необходимой для успешной деятельности фирмы в условиях конкуренции. Непосредственно добыванием информации о конкуренте занимается группа обеспечения внешней деятельности организации.

Некоторые сведения о деятельности конкурентов можно легко получить из легальных источников – средств массовой информации, деловых контактов, научно-практических конференций и т.п. Как правило, такие сведения не раскрывают всех особенностей деятельности конкурента, особенно секретов производства, и не могут нанести серьезный ущерб. Объектами промышленного шпионажа чаще всего являются: технологические процессы существующего и перспективного производства продукции, результаты научно-исследовательских работ, ноу-хау, характеристики маркетинговой политики. Эти сведения фирмы должны надежно защищать.

Один из способов подбора кандидатов на роль промышленного шпиона заключается в организации с ним беседы о якобы выборе претендента на престижную работу. В случае согласия на следующем этапе следуют конкретные предложения по участию в промышленном шпионаже.

Существуют и другие методы вербовки промышленных шпионов. Чаще всего для вербовки применяются шантаж и подкуп сотрудников фирмы, имеющих легальный доступ к интересующей информации.

Промышленные шпионы применяют различные методы сбора информации, в том числе и находящиеся на вооружении спецслужб различных государств:

- агентурный шпионаж;
- технические средства разведки;
- негласный сбор информации из содержимого мусорных корзин;
- получение определенного объема информации из доступных источников – публикаций в ведомственных журналах, в органах контроля за деятельностью предприятий, материалов конференций, выставок, рекламных материалов и т.п.;
- банки данных о предприятиях и фирмах, которые создаются акционерными обществами, малыми предприятиями и кооперативами;
- обратный инжиниринг, т.е. анализ и изучение продукции конкурентов с целью исследования конструкции, технологии и других характеристик изделий;
- непосредственное наблюдение за работой конкурирующего предприятия;
- годовые отчеты фирм, предприятий, в том числе подготовленные для своих акционеров и представляющие коммерческую тайну;
- отчеты торговых агентов и посредников предприятия о спросе на производимую продукцию, о масштабах производства аналогичной продукции конкурентами и т. п.

Добытые разведкой разрозненные сведения не всегда дают полное представление о реальной деятельности конкурентов. Поэтому важнейшее значение имеет информационно-аналитическая служба, которая занимается анализом добытых сведений и прогнозированием возможных ситуаций.

Агентурный шпионаж и сейчас остается наиболее эффективным методом негласного сбора информации. Если он по каким-либо причинам невозможен, то прибегают к другим методам, в частности к добыванию информации с применением технических средств. Преимуществом такого метода является относительно небольшой риск разоблачения агента, добывающего информацию.

Одним из важных средств добывания информации является техническая разведка, проводимая с помощью разнообразных специальных техни-

ческих устройств. Вид применяемых технических средств разведки зависит прежде всего от физической природы источников информационных сигналов, носителей информации, особенностей демаскирующих признаков объектов.

Дистанционное добывание информации позволяет съем ее с носителей, доступ к которым возможен из-за пределов контролируемой зоны. Оно возможно в результате наблюдения, прослушивания, перехвата, сбора материальных носителей информации (бракованных изделий, демаскирующих веществ и др.).

Сбор содержимого мусорных корзин, содержащих технологические отходы, образовавшиеся в результате обработки охраняемой законом информации, относится к негласным методам сбора информации. В мусорных корзинах могут оказаться испорченные или недоработанные документы, черновые варианты производственных планов, испорченные диски и т.п. Если содержимое мусорных корзин не уничтожено надлежащим образом, то по нему может быть восстановлена исходная информация.

В-4. Задачи систем защиты информации

Защита информации представляет собой комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.

Под системой защиты информации можно понимать государственную систему защиты информации и систему защиты информации на конкретных объектах.

Государственная система защиты информации включает в себя:

- систему государственных нормативных актов, стандартов, руководящих документов и требований;
- разработку концепций, требований, нормативно-технических документов и научно-методических рекомендаций по защите информации;
- порядок организации, функционирования и контроля за выполнением мер, направленных на защиту информации, являющейся собственностью государства, а также рекомендаций по защите информации, находящейся в собственности физических и юридических лиц;
- организацию испытаний и сертификации средств защиты информации;
- создание ведомственных и отраслевых координационных структур для защиты информации;
- осуществление контроля за выполнением работ по организации защиты информации;
- определение порядка доступа юридических и физических лиц иностранных государств к информации, являющейся собственностью государства, или к информации физических и юридических лиц, относительно распространения и использования которой государством установлены ограничения.

Цели защиты информации от технических средств разведки на конкретных объектах информатизации определяются конкретным перечнем потенциальных угроз. В общем случае цели защиты информации можно сформулировать как:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется ее своевременностью, активностью, непрерывностью и комплексностью. Очень важно проводить защитные мероприятия комплексно, то есть обеспечивать нейтрализацию всех опасных каналов утечки информации. Необходимо помнить, что даже один-единственный не закрытый канал утечки может свести на нет эффективность системы защиты.

1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

1.1. Общие понятия

Основными объектами защиты информации являются [1]:

- Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.
- Средства и информационные системы (средства вычислительной техники, сети и системы), программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. Эти средства и системы часто называют техническими средствами приёма, обработки и хранения информации (ТСПИ).
- Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.
- ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

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

1.2. Технические каналы утечки информации. Структура, классификация и основные характеристики

Наибольший интерес с точки зрения образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие выход за пределы *контролируемой зоны* (КЗ), т.е. зоны с пропускной системой. Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС (рис. 1.1).

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

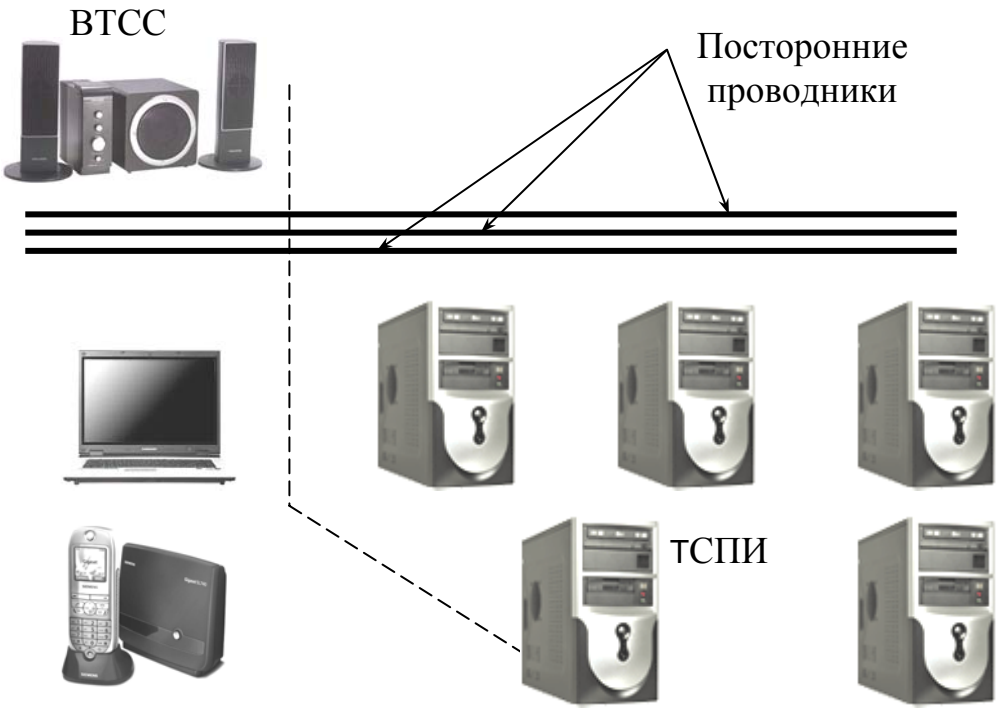


Рис. 1.1. Источники образования возможных каналов утечки информации

Случайными антеннами могут быть цепи ВТСС или посторонние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ. Случайные антенны бывают сосредоточенными и распределёнными. Сосредоточенная случайная антенна представляет собой техническое средство с сосредоточенными параметрами (телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д.). Распределённые случайные антенны образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

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

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал (рис. 1.2). В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте [1].

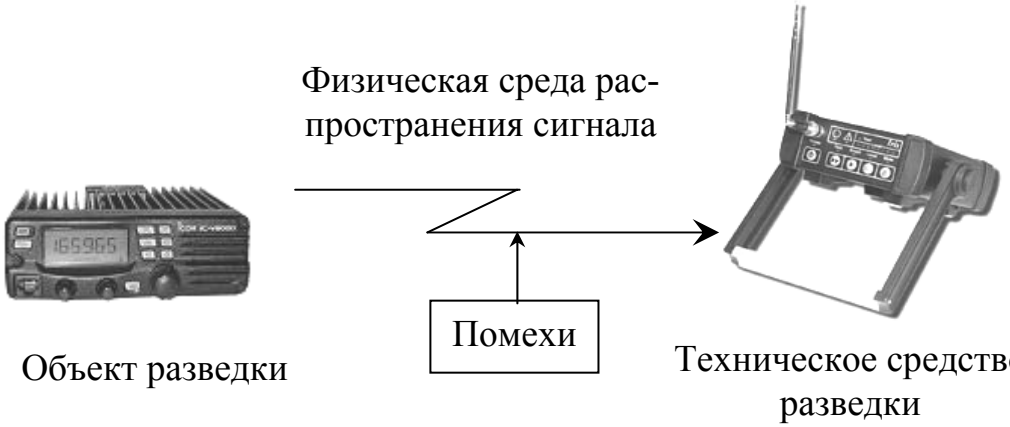


Рис. 1.2. Технический канал утечки информации (ТКУИ)

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

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

Классификация каналов утечки информации представлена на рис. 1.3.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов утекаемой информации. Ниже приведены некоторые особенности технических каналов утечки информации.

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:

- электромагнитные излучения элементов ТСПИ;
- электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
- излучения на частотах самовозбуждения усилителей низкой частоты.

2. Электрические:

- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
- просачивание информационных сигналов в линии электропитания;
- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

3. Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ.

4. Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

• электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

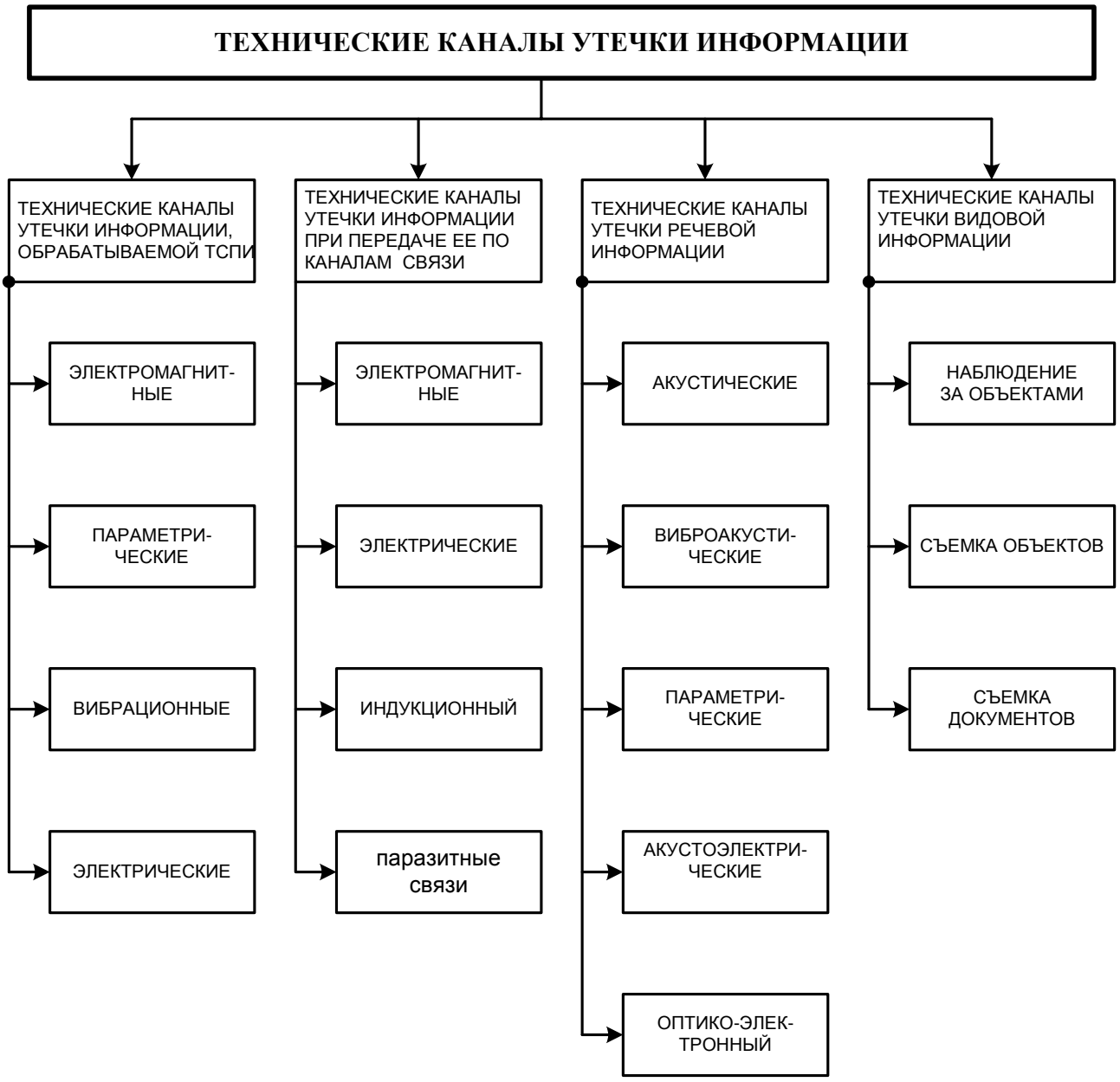


Рис. 1.3. Технические каналы утечки информации

2. Электрические каналы:

• подключение к линиям связи.

3. Индукционный канал:

• эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

- паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

- среда распространения – воздух.

2. Виброакустические каналы:

- среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:

- результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:

- преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:

- облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами.

Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съемка объектов.

Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3. Съемка документов.

Съемка документов осуществляется с использованием портативных фотоаппаратов

1.2.1. Технические каналы утечки информации, обрабатываемой ТСПИ

Электромагнитные каналы утечки информации

Основным каналом утечки информации при ее обработке ТСПИ является электромагнитный канал, обусловленный побочными информативными электромагнитными излучениями основных технических средств обработки информации. К *электромагнитным* относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ТСПИ. Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона,

создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

Рассмотрим некоторые особенности и свойства электромагнитных каналов.

1.2.1.1. Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля

Электромагнитное поле представляет собой особый вид материи. Оно, как и вещество, обладает не только энергией, но также массой, количеством движения и моментом количества движения. Поле может превращаться в вещество, как и вещество – в поле. Электромагнитное поле воздействует с определенной силой на заряженные частицы.

Электромагнитное поле определяется во всех точках двумя векторными величинами – электрическим полем и магнитным полем. Электрическое поле характеризуется воздействием на электрически заряженную частицу с силой, пропорциональной заряду частицы и не зависящей от ее скорости. Магнитное поле воздействует на движущуюся частицу с силой, пропорциональной заряду частицы и ее скорости.

Для расчета электромагнитного поля наиболее пригодны уравнения электродинамики в интегральной и дифференциальной формах [35].

Электромагнитное поле характеризуется четырьмя векторными величинами: $\vec{E}$ – напряженность электрического поля (В/м); $\vec{D}$ – электрическая индукция (вектор электрического смещения) ((Кл/м^2); $\vec{H}$ – напряженность магнитного поля (А/м); $\vec{B}$ – магнитная индукция (Тл).

Определение поля в некоторой области пространства требует указания этих векторов в любой ее точке. В общем случае взаимосвязь векторов электромагнитного поля определяется свойствами среды:

$$\vec{D} = \varepsilon \vec{E}; \qquad (1.1)$$

$$\vec{B} = \mu \vec{H}, \qquad (1.2)$$

где $\varepsilon = \varepsilon_r \varepsilon_0$ – диэлектрическая проницаемость среды; $\varepsilon_0 = 8{,}855 \cdot 10^{-12}$ – диэлектрическая проницаемость вакуума (Ф/м); ε_r – относительная диэлектрическая проницаемость среды, в которой находятся заряды; $\mu = \mu_r \mu_0$ – абсолютная магнитная проницаемость среды; $\mu_0 = 4\pi \cdot 10^{-7}$ – магнитная проницаемость вакуума (Гн/м); μ_r – относительная магнитная проницаемость среды.

Безразмерные величины ε_r и μ_r для воздушной среды близки к единице. Например, для воздушной среды при температуре 0° $\varepsilon_r = 1{,}0006$.

Основными уравнениями электромагнитного поля являются уравнения Максвелла. Первое уравнение Максвелла соответствует вихрям магнитного поля и относится к одному из основных уравнений электродинамики:

$$\mathrm{rot}\,\vec{H} = \vec{\delta} + \frac{\partial \vec{D}}{\partial t}. \qquad (1.3)$$

Физический смысл этого уравнения можно толковать следующим образом: магнитное поле возбуждается совместным действием тока проводимости с плотностью $\vec{\delta}$ и изменением во времени электрического поля (вектора электрического смещения $\vec{D}$). Величина $\frac{\partial \vec{D}}{\partial t}$ называется плотностью тока смещения. Вектор $\vec{\delta}$ указывает направление движения зарядов и по абсолютному значению равен пределу

$$\vec{\delta} = \lim_{\Delta S \to 0} \frac{\Delta I}{\Delta S}, \qquad (1.4)$$

где ΔI – ток через площадку ΔS, перпендикулярную $\vec{\delta}$. Плотность тока проводимости $\vec{\delta} = \gamma \vec{E},$ где γ – удельная проводимость.

Сумму $\vec{\delta} + \frac{\partial \vec{D}}{\partial t}$ называют плотностью полного тока.

Второе уравнение Максвелла выражает скорость изменения магнитной индукции $\vec{B}$ через пространственную производную (rot) напряженности электрического поля $\vec{E}$:

$$\mathrm{rot}\,\vec{E} = -\frac{\partial \vec{B}}{\partial t}. \qquad \textbf{(1.5)}$$

Физический смысл второго уравнения Максвелла состоит в том, что электрическое поле может возбуждаться не только электрическими зарядами, но и изменениями во времени магнитного поля (вектора магнитной индукции $\vec{B}$).

Если изобразить в пространстве произвольную поверхность S с контуром L (рис. 1.4), то можно определить поток вектора $\mathrm{rot}\,\vec{E}$ через эту поверхность.

Согласно (1.5) имеем:

$$\int_S \mathrm{rot}\,\vec{E}\,d\vec{S} = -\int_S \frac{\partial \vec{B}}{\partial t} d\vec{S}. \qquad \textbf{(1.6)}$$

Векторный символ $d\vec{S}$ обозначает произведение элемента поверхности dS на единичный вектор нормали к ней $\vec{n}_0$.

Применяя теорему Стокса ($\int_S \mathrm{rot}\,\vec{v}\,dV = \oint_L \vec{v}\,d\vec{l}$, где $\vec{v}$ – любой вектор) и вынося оператор временной производной за знак интеграла заменим поток вихря $rot\,\vec{E}$ циркуляцией вектора $\vec{E}$ по контуру, охватывающему поток:

$$\oint_L \vec{E} d\vec{l} = -\frac{\partial}{\partial t} \int_S \vec{B} d\vec{S}, \qquad \textbf{(1.7)}$$

где $d\vec{l}$ – произведение элемента линии *dl* на касательный к ней единичный вектор $\vec{\tau}_0$.

Уравнение (1.7) представляет собой второе уравнение Максвелла в интегральной форме.

Если поверхность *S* (рис. 1.5) опирается на проводящий контур *L* (например, проволочный), то выражение (1.7) можно записать как

$$e = -\frac{\partial \Phi}{\partial t}, \qquad (1.8)$$

где циркуляция вектора $\vec{E}$ в этом случае есть не что иное, как ЭДС $e = \oint_L \vec{E} d\vec{l}$, наводимая в контуре изменяющимся потоком вектора магнитной индукции, а $-\frac{\partial}{\partial t} \int_S \vec{B} d\vec{S} = -\frac{d\Phi}{dt}$, где Φ – магнитный поток. В итоге для рассматриваемого случая имеем хорошо известный закон электромагнитной индукции: $e = -\frac{d\Phi}{dt}$.

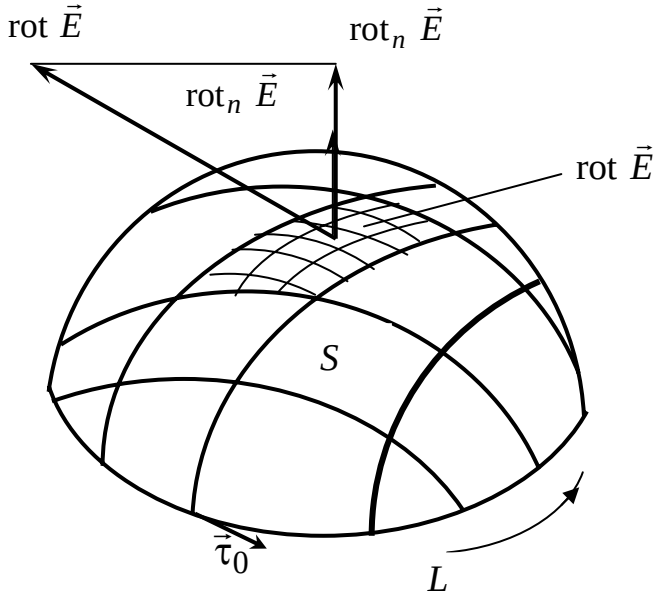


Рис. 1.4

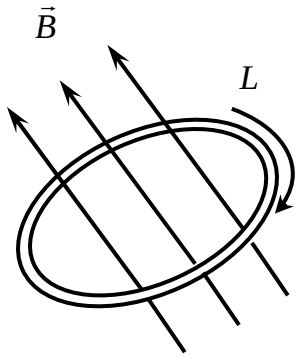


Рис. 1.5

Второе уравнение Максвелла можно рассматривать как обобщенный закон электромагнитной индукции.

Интегральная форма первого уравнения Максвелла может быть получена интегрированием обеих частей уравнения (1.3) по произвольной поверхности *S* с контуром *L* и применением теоремы Стокса:

$$\oint_L \vec{H} d\vec{l} = \frac{\partial}{\partial t} \int_S \vec{D} d\vec{S} + \int_S \vec{\delta} d\vec{S}. \qquad (1.9)$$

Интеграл $\int_S \vec{\delta} d\vec{S} = I$ – поток вектора $\vec{\delta}$ через поверхность S – является током проводимости, пересекающим эту поверхность, а составляющая $\frac{\partial}{\partial t}\int_S \vec{D} d\vec{S} = I_{\text{см}}$ – ток смещения. Сумма $I + I_{\text{см}}$ называется полным током.

К основным уравнениям Максвелла относят также следующие два уравнения в дифференциальной форме:

$$\operatorname{div}\vec{D} = \rho; \tag{1.10}$$

$$\operatorname{div}\vec{B} = 0. \tag{1.11}$$

Согласно первому уравнению расходимость электрической индукции равна объемной плотности заряда ρ – величине, определяемой предельным соотношением:

$$\rho = \lim_{\Delta V \to 0} \frac{\Delta q}{\Delta V}, \tag{1.12}$$

где Δq – заряд, содержащийся в элементарном объеме ΔV.

Интегрированием обеих частей уравнения (1.10) по некоторому объему V и применением к левой части формулы Остроградского-Гаусса получим

$$\oint_S \vec{D} d\vec{S} = q. \tag{1.13}$$

Здесь S – поверхность, ограничивающая объем V, а $q = \int_V \rho dV$ – полный заряд в этом объеме.

Равенство (1.13) является интегральной формой уравнения Максвелла (1.10) и является формулировкой теоремы Гаусса: поток электрической индукции через замкнутую поверхность равен заключенному внутри ее заряду.

Интегральную форму уравнения (1.11) получают интегрированием $\operatorname{div}\vec{B}$ по объему V и применением формулы Остроградского-Гаусса:

$$\oint_S \vec{B} d\vec{S} = 0. \tag{1.14}$$

В заключение приведем систему уравнений Максвелла в дифференциальной и интегральной формах.

Интегральная форма:

$$\begin{gathered}
\oint_L \vec{H} d\vec{l} = \frac{d}{dt}\int_S \vec{D} d\vec{S} + \int_S \vec{\delta} d\vec{S}, \\
\oint_L \vec{E} d\vec{l} = -\frac{d}{dt}\int_S \vec{B} d\vec{S}, \ \oint_S \vec{D} d\vec{S} = q, \\
\oint_S \vec{B} d\vec{S} = 0.
\end{gathered} \tag{1.15}$$

Дифференциальная форма:

$$\begin{aligned}
&\operatorname{rot}\vec{H} = \frac{\partial \vec{D}}{\partial t} + \vec{\delta},\\
&\operatorname{rot}\vec{E} = -\frac{\partial \vec{B}}{\partial t},\\
&\operatorname{div}\vec{D} = \rho,\\
&\operatorname{div}\vec{B} = 0,\\
&\vec{B} = \mu\vec{H},\\
&\vec{D} = \varepsilon\vec{E},\\
&\vec{\delta} = \gamma\vec{E}.
\end{aligned} \qquad (1.16)$$

Преобразованием (исключением $\vec{D}$ и $\vec{B}$) систему уравнений (1.16) можно привести к форме, в которой переменными будут только напряженности электрического и магнитного полей:

$$\operatorname{rot}\vec{H} = \varepsilon_r\varepsilon_0\frac{\partial \vec{E}}{\partial t} + \vec{\delta},\ \operatorname{rot}\vec{E} = -\mu_r\mu_0\frac{\partial \vec{H}}{\partial t},\ \operatorname{div}\vec{E} = \frac{\rho}{\varepsilon_r\varepsilon_0}\ (\varepsilon_r = \text{const}),$$
$$\operatorname{div}\vec{H} = 0\ (\mu_r = \text{const}),\ \vec{\delta} = \gamma\vec{E}\ (\text{при}\ \vec{E}_{\text{стор}} = 0). \qquad (1.17)$$

Системы уравнений (1.15)…(1.17) являются исходными при изучении электромагнитного поля.

Для радиотехники переменное электромагнитное поле представляет основной интерес. Для изучения установившихся электромагнитных процессов, которые характеризуются гармоническими во времени колебаниями, всякую характеризующую поле скалярную величину можно представить как $\psi = \psi_m\cos(\omega t + \varphi_\psi)$. Тогда всякий вектор поля $\vec{V}$ разлагается на компоненты, изменяющиеся по аналогичному закону:

$$\vec{V} = \vec{a}_1 V_{1m}\cos(\omega t + \varphi_1) + \vec{a}_2 V_{2m}\cos(\omega t + \varphi_2) + \vec{a}_3 V_{3m}\cos(\omega t + \varphi_3), \qquad (1.18)$$

где $\vec{a}_1, \vec{a}_2, \vec{a}_3$ – орты некоторой системы координат q_1, q_2, q_3.

Величина $\omega = 2\pi f$ называется круговой частотой гармонических колебаний; ψ_m и V_{im} – амплитуды, φ_ψ и φ_i – начальные фазы.

Анализ гармонических процессов значительно упрощается применением метода комплексных амплитуд, когда изображающий вектор рассматривается на комплексной плоскости. По формуле Эйлера

$$e^{j(\omega t+\varphi)} = \cos(\omega t + \varphi) + j\sin(\omega t + \varphi)$$

видно, что скаляр ψ (см. выше) и вектор $\vec{V}$ можно выразить как вещественные части величин

$$\dot{\psi} = \psi_m e^{j(\omega t+\varphi_\psi)};$$
$$\dot{\vec{V}} = \vec{a}_1 V_{1m} e^{j(\omega t+\varphi_1)} + \vec{a}_2 V_{2m} e^{j(\omega t+\varphi_2)} + \vec{a}_3 V_{3m} e^{j(\omega t+\varphi_3)}, \quad (1.19)$$

которые называются их комплексами. В (1.19) $\vec{a}_1, \vec{a}_2, \vec{a}_3$ – орты некоторой системы координат. Таким образом $\vec{\psi} = \mathrm{Re}\,\dot{\psi}$, $\vec{V} = \mathrm{Re}\,\dot{V}$.

Выделим в комплексе $\dot{\vec{V}}$ множитель

$$\dot{\vec{V}} = \vec{a}_1 V_{1m} e^{j\varphi_1} + \vec{a}_2 V_{2m} e^{j\varphi_2} + \vec{a}_3 V_{3m} e^{j\varphi_3}, \quad (1.20)$$

который называют комплексной амплитудой. Через комплексную амплитуду можно выразить комплекс $\dot{\vec{V}}$ как $\dot{\vec{V}} = \dot{\vec{V}}_m e^{j\omega t}$. Дифференцирование комплекса по времени соответствует его умножение на $j\omega$.

Если комплекс $\dot{\vec{V}}$ удовлетворяет некоторому линейному дифференциальному уравнению, то данному уравнению удовлетворяют его вещественная и мнимая части.

С учетом приведенных выше соотношений уравнения Максвелла (1.17) в комплексных значениях принимают форму:

$$\begin{aligned}
&\mathrm{rot}\,\dot{\vec{H}}_m = \dot{\vec{\delta}}_m + j\omega\varepsilon_r\varepsilon_0\dot{\vec{E}}_m;\\
&\mathrm{rot}\,\dot{\vec{E}}_m = -j\omega\mu_r\mu_0\dot{\vec{H}}_m;\\
&\mathrm{div}\,\dot{\vec{H}}_m = 0; \quad (1.21)\\
&\mathrm{div}\,\dot{\vec{E}}_m = \frac{\dot{\rho}_m}{\varepsilon_r\varepsilon_0};\\
&\dot{\vec{\delta}}_m = \gamma\dot{\vec{E}}_m.
\end{aligned}$$

Уравнения (1.21) могут быть упрощены, если учесть, что

$$\varepsilon_r = 1{,}0006.$$

Рассмотрим некоторую область V (рис. 1.6), в которой распределен заряд ($\rho \neq 0$) и присутствует ток ($\vec{\delta} \neq 0$). В некоторой точке M существует электрическое поле, потенциал которого φ есть решение уравнения Пуассона

$$\frac{\partial^2\varphi}{\partial x^2} + \frac{\partial^2\varphi}{\partial y^2} + \frac{\partial^2\varphi}{\partial z^2} = -\frac{\rho}{\varepsilon} \quad (1.22)$$

и выражается формулой

$$\varphi = \frac{1}{4\pi\varepsilon}\int_V \frac{1}{r}\rho\,dV, \quad (1.23)$$

а также магнитное поле, характеризуемое векторным потенциалом $\vec{A}$, определяемым из решения уравнения $\nabla^2\vec{A} = -\mu\vec{\delta}$ как

$$\vec{A}=\frac{\mu}{4\pi}\int_V\frac{1}{r}\vec{\delta}dV,$$

где $\nabla=\vec{x}_0\frac{\partial}{\partial x}+\vec{y}_0\frac{\partial}{\partial y}+\vec{z}_0\frac{\partial}{\partial z}$ – оператор Гамильтона.

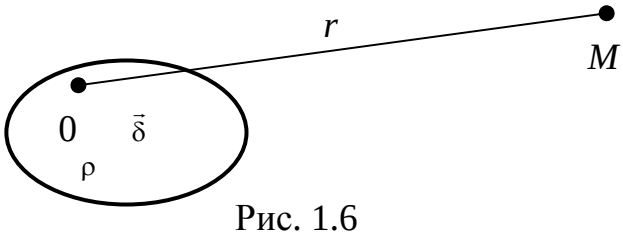


Рис. 1.6

Для решения системы уравнений (1.21) необходимо определить для электромагнитного поля электрический φ и магнитный A запаздывающие потенциалы:

$$\begin{aligned}\varphi(t)&=\frac{1}{4\pi\varepsilon}\int_V\frac{1}{r}\rho(t-\frac{r}{v})dV,\\ \vec{A}(t)&=\frac{\mu}{4\pi}\int_V\frac{1}{r}\vec{\delta}(t-\frac{r}{v})dV,\end{aligned}\qquad(1.24)$$

где r – расстояние до точки наблюдения M; v – фазовая скорость бегущей волны, связанная с постоянной распространения волны в неограниченном пространстве k соотношением $k=\frac{\omega}{v}$. Величины ρ и $\vec{\delta}$ связаны между собой уравнением

$$div\vec{\delta}=-\frac{d\rho}{dt}.\qquad(1.25)$$

В комплексной форме выражения запаздывающих потенциалов принимают вид:

$$\begin{aligned}\dot{\varphi}_m&=\frac{1}{4\pi\varepsilon}\int_V\dot{\rho}\frac{e^{-jkr}}{r}dV,\\ \dot{\vec{A}}&=\frac{\mu}{4\pi}\int_V\dot{\vec{\delta}}\frac{e^{-jkr}}{r}dV.\end{aligned}\qquad(1.26)$$

Если рассматривать поле, создаваемое одним лишь колеблющимся зарядом $q=\rho_m\Delta V\cos\omega t=q_m\cos\omega t$, расположенным в пространстве ΔV, то согласно (1.26) комплексная амплитуда потенциала этого поля будет

$$\dot{\varphi}_m=\frac{\dot{q}_m}{4\pi\varepsilon}\cdot\frac{e^{-jkr}}{r},\qquad(1.27)$$

а сам потенциал равен:

$$\varphi=\frac{q_m}{4\pi\varepsilon r}\cos(\omega t-kr).\qquad(1.28)$$

В этом случае поле имеет форму сферической волны, расходящейся из точки, в которой расположен заряд, со скоростью *v*.

С учетом параметров *A* и φ напряженности магнитного и электрического полей можно выразить как

$$\vec{H} = \frac{1}{\mu\mu_0}\operatorname{rot}\vec{A};$$
$$\vec{E} = -\frac{\partial\vec{A}}{\partial t} - \operatorname{grad}\varphi, \qquad (1.29)$$

где

$$\operatorname{grad}\varphi = \begin{cases} \dfrac{d\varphi}{dx} \\ \dfrac{d\varphi}{dy} \\ \dfrac{d\varphi}{dz} \end{cases}$$

1.2.1.2. Элементарный электрический излучатель

Диполь, момент которого изменяется во времени, называют элементарным излучателем. Различают электрический и магнитный излучатели: электрический и магнитный диполи. Диполь, момент которого изменяется по синусоидальному закону, называют гармоническим.

Электрический излучатель соответствует элементу электрического тока. В этом легко убедиться, если рассмотреть производную по времени от момента электрического диполя. Так как электрический момент (векторная величина) $\vec{p} = q\vec{l}$, то $\frac{\partial\vec{p}}{\partial t} = \frac{\partial q}{\partial t}\vec{l} = I\vec{l}$, при этом положительное направление тока *I* совпадает с $\vec{p}$.

По аналогии производная по времени от момента замкнутого витка с током $\vec{m} = -\mu I\vec{S}$ магнитного диполя соответствует элементу магнитного тока $\frac{\partial\vec{m}}{\partial t} = -\mu\vec{S}\frac{\partial I}{\partial t}$.

Рассмотрим элементарный электрический излучатель. Для этого представим отрезок проводника *l*, ориентированный вдоль координатной оси *z* и по которому течет ток $I = I_m\cos\omega t$ (рис. 1.7).

В [35] показано, что при условии постоянства амплитуды тока вдоль всего участка можно условно полагать сосредоточение равных по

абсолютной величине и противоположных по знаку колеблющихся зарядов (рис. 1.8) с комплексными амплитудами

$$\dot{q}_m = \pm \frac{jI_m}{\omega}. \tag{1.30}$$

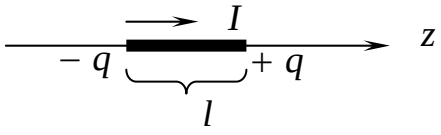


Рис. 1.7

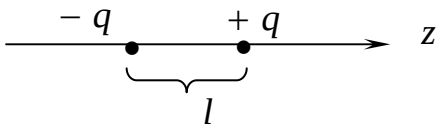


Рис. 1.8

Это значит, что рассматриваемый отрезок с током можно представить как диполь, момент которого $\dot{\vec{p}}_m = \vec{z}_0 lq$ совершает гармонические колебания с частотой ω и имеет комплексную амплитуду

$$\dot{\vec{p}}_m = -j\frac{I_m l}{\omega}\vec{z}_0. \tag{1.31}$$

Изображенный на рис. 1.7 элемент тока (колеблющийся диполь) рассматривается в качестве элементарного излучателя и называется диполем Герца.

Расположив диполь в сферической системе координат (рис. 1.9) получают комплексную амплитуду векторного потенциала элемента тока:

$$\dot{\vec{A}}_m = (\vec{r}_0 \cos\vartheta - \vec{\vartheta}_0 \sin\vartheta)\frac{\mu l I_m}{4\pi r} e^{-jkr}. \tag{1.32}$$

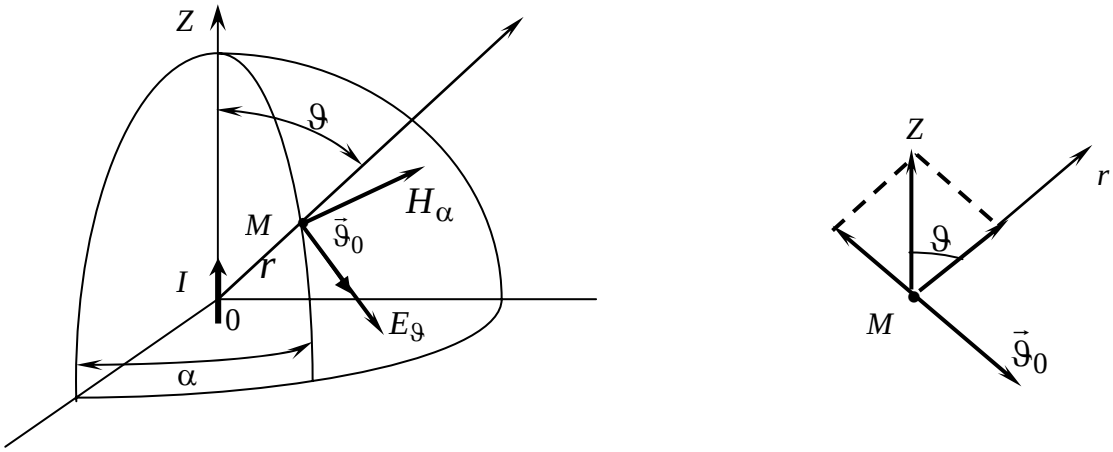


Рис. 1.9

Компоненты поля, создаваемого диполем Герца в произвольной точке пространства $M(r, \vartheta, \alpha)$, определяются по приведенным выше формулам и при переходе от комплексов к векторам поля принимают вид:

$$H_\alpha = \frac{klI_m}{4\pi r}[\frac{1}{kr}\cos(\omega t - kr) - \sin(\omega t - kr)]\sin\vartheta;$$

$$E_r = \frac{klI_m}{2\pi\omega\varepsilon r^2}[\frac{1}{kr}\sin(\omega t - kr) + \cos(\omega t - kr)]\cos\vartheta; \qquad (1.33)$$

$$E_\vartheta = \frac{k^2 lI_m}{4\pi\omega\varepsilon r}[(\frac{1}{k^2 r^2} - 1)\sin(\omega t - kr) + \frac{1}{kr}\cos(\omega t - kr)]\sin\vartheta;$$

$$H_r = H_\vartheta = E_\alpha = 0.$$

Ближняя зона (зона квазистационарности). Границы этой зоны определяются условиями $r \gg l$ (l – длина элемента тока или плечо вибратора) и $kr \ll 1$, или $r \ll 1/k$. В силу равенства $k = 2\pi/\lambda$ второе условие принимает вид $r \ll \lambda/2\pi$ (условие квазистационарности). Для ближней зоны (на расстояниях от вибратора существенно меньших длины волны) формулы (1.33) можно упростить, отбрасывая малые члены в квадратных скобках и пренебрегая фазовым сдвигом kr:

$$H_\alpha = \frac{lI_m}{4\pi r^2}\sin\vartheta\cos\omega t; \quad E_r = \frac{p_m}{2\pi\varepsilon r^3}\cos\vartheta\sin\omega t;$$

$$E_\vartheta = \frac{p_m}{4\pi\varepsilon r^3}\sin\vartheta\sin\omega t; \quad p_m = \frac{lI_m}{\omega}. \qquad (1.34)$$

Поле согласно (1.34) не имеет волнового характера, так как выражения (1.34) получены в пренебрежении излучением в ближней зоне вследствие его незначительности. Пространственное распределение в этом случае свойственно статическому диполю. Выражения (1.34) содержат одну составляющую вектора напряженности магнитного поля элемента тока и две составляющие вектора напряженности электрического поля вибратора, характеризующиеся в каждый момент времени как «стационарные» величины. Из (1.34) следует, что величины E и H сдвинуты по фазе на угол 90°.

Дальняя зона. Рассмотрим поле на расстояниях, значительно превышающих длину волны, когда $r \gg \lambda$ и $kr \gg 1$. В этом случае можно пренебречь членами порядка $1/k^2 r^2$ и $1/kr$. Тогда уравнения (1.33) принимают вид [35]:

$$H_\alpha = -\frac{klI_m}{4\pi r}\sin\vartheta\sin(\omega t - kr);$$

$$E_r = 0; \qquad (1.35)$$

$$E_\vartheta = -\frac{klW^0 I_m}{4\pi r}\sin\vartheta\sin(\omega t - kr).$$

В (1.35) введено отношение амплитуд E_m и H_m, которое равно $W^0 = \frac{E_m}{H_m} = \sqrt{\frac{\mu}{\varepsilon}}$ и называется волновым сопротивлением неограниченной среды. Для вакуума $W^0 = \sqrt{\frac{\mu_0}{\varepsilon_0}} = 120\pi$ [Ом].

Уравнения (1.35) соответствуют полю излучения. Оно представляет собой сферическую волну. Векторы $\vec{E}$ и $\vec{H}$ расположены перпендикулярно к направлению распространения волны, взаимно перпендикулярны и синфазны. Излучение максимально в экваториальной плоскости ($\vartheta = 90°$) и отсутствует в осевом направлении ($\vartheta = 0$).

Более полное представление об излучении дает диаграмма направленности (рис. 1.10), которую изображают следующим построением. В произвольной меридиональной плоскости откладываются ряд отрезков, пропорциональных амплитуде E_m (или H_m) в данном направлении ϑ для фиксированного расстояния r. Концы этих отрезков будут лежать на двух соприкасающихся окружностях. Полная мощность, излучаемая диполем Герца, определяется выражением

$$\vec{P} = \frac{\pi}{3} I_m^2 W^0 (\frac{l}{\lambda})^2. \qquad (1.36)$$

Оно показывает, что излучение резко возрастает при ослаблении условия квазистационарности поля ($l << \lambda$).

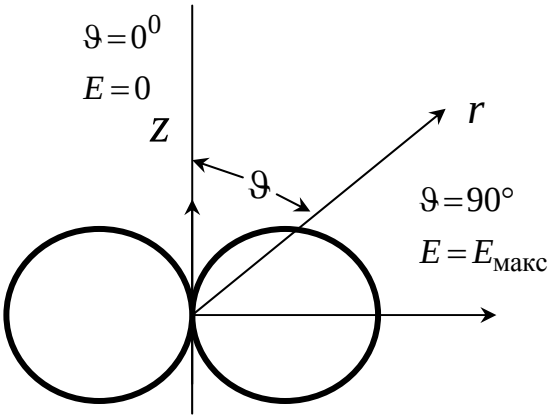


Рис. 1.10. Диаграмма направленности

1.2.1.3. Элементарный магнитный излучатель

В теории электромагнитного поля доказывается [35], что замкнутый виток (рис. 1.11, *а*) с постоянным током на превышающих его размеры расстояниях создает такое же магнитное поле как если бы на его месте находился магнитный диполь (рис. 1.11, *б*) с моментом $\vec{m} = \vec{z}_0 I \mu S$.

При гармоническом токе витка $I = I_m \cos\omega t$ переменный магнитный диполь характеризуется комплексной амплитудой момента $\dot{\vec{m}} = \vec{z}_0 \dot{I}_m \mu S$. Такой виток называют элементарным магнитным излучателем или магнитным диполем Герца.

Решение уравнений Максвелла для магнитного диполя Герца в комплексной форме имеет вид

$$\dot{\vec{E}} = -\vec{\alpha}_0 \frac{j\omega\mu I_m S}{4\pi r}\left(\frac{1}{r} + jk\right)e^{j(\omega t - kr)}\sin\vartheta;$$
$$\dot{\vec{H}} = \frac{I_m S}{4\pi}\left[\vec{r}_0 \frac{2}{r^2}\left(\frac{1}{r} + jk\right)\cos\vartheta + \vec{\vartheta}_0 \frac{1}{r}\left(\frac{1}{r^2} + j\frac{k}{r} - k^2\right)\sin\vartheta\right]e^{j(\omega t - kr)}. \quad (1.37)$$

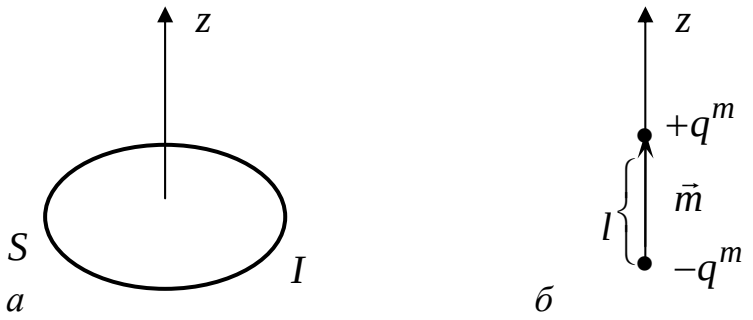


Рис. 1.11

Из (1.37) определяется запись компонент электромагнитного поля:

$$E_\alpha = \frac{I_m k^2 S W^0}{4\pi r}\left[\frac{1}{kr}\sin(\omega t - kr) + \cos(\omega t - kr)\right]\sin\vartheta;$$
$$H_r = \frac{I_m k S}{2\pi r^2}\left[\frac{1}{kr}\cos(\omega t - kr) - \sin(\omega t - kr)\right]\cos\vartheta; \quad (1.38)$$
$$H_\vartheta = \frac{I_m k^2 S}{4\pi r}\left[\left(\frac{1}{k^2 r^2} - 1\right)\cos(\omega t - kr) - \frac{1}{kr}\sin(\omega t - kr)\right]\sin\vartheta;$$
$$E_r = E_\vartheta = H_\alpha = 0.$$

Сравнивая (1.33) и (1.38) отмечаем, что уравнения Максвелла характеризуются перестановочной двойственностью.

Из (1.38) получаем компоненты ближнего поля:

$$E_\alpha = \frac{I_m \mu S \omega}{4\pi r^2}\sin\vartheta\sin\omega t; \quad H_r = \frac{m_m}{2\pi\mu r^3}\cos\vartheta\cos\omega t;$$
$$H_\vartheta = \frac{m_m}{4\pi\mu r^3}\cos\vartheta\cos\omega t; \quad m_m = I_m \mu S \quad (1.39)$$

и поля излучения:

$$E_\alpha = \frac{I_m k^2 S W^0}{4\pi r}\cos(\omega t - kr)\sin\vartheta;\ \ H_r = 0;$$
$$H_\vartheta = -\frac{I_m k^2 S}{4\pi r}\cos(\omega t - kr)\sin\vartheta. \qquad (1.40)$$

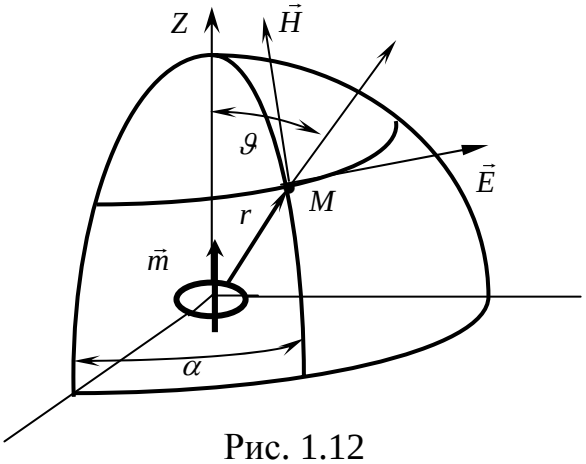


Рис. 1.12

В дальней зоне элементарный магнитный излучатель создает волновое поле, которое отличается от поля элементарного электрического излучателя только ориентацией (рис. 1.12). Диаграмма направленности магнитного излучателя не отличается от диаграммы направленности элементарного электрического излучателя (рис. 1.10).

1.2.1.4. Электромагнитные каналы утечки информации ТСПИ

К побочным электромагнитным излучениям ТСПИ относятся:

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

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

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватывать-

ся портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

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

Электромагнитные излучения персональных компьютеров. Согласно оценочным данным по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1–2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ) [33]. На первый взгляд может показаться, что этот канал менее опасен по сравнению, например, с акустическим, по которому из помещения может быть перехвачена речевая информации в полном объеме. Но необходимо помнить, что в настоящее время наиболее важная информация, содержащая государственную тайну или технологические секреты, обрабатывается на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе.

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

Аналогичная ситуация имеет место и при взаимном обмене сигналами между параллельно проложенными кабелями. Исследователями продемонстрировано восстановление сетевых данных через телефонную линию, причем телефонный кабель проходил рядом с кабелем компьютерной сети всего на протяжении двух метров. Еще одна опасность исходит от "активных" атак (высокочастотное навязывание): злоумышленник, знающий резонансную частоту, например, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте, а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса.

Для ПК высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50–300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательностей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах высокочастотной коммутации.

Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, так как расположение его составных частей имеет много комбинаций. ПК имеет линейную поляризацию. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке.

Уровни побочных электромагнитных излучений ВТ регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации «№ 22 CISPR (специальный международный комитет по радиопомехам) для диапазона 230–1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием ВТ, на расстоянии 10 м не должен превышать 37 дБ. Однако излучения такого уровня могут быть перехвачены на значительных расстояниях. Следовательно, соответствие электромагнитных излучений средств ВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности обрабатываемой в них информации.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы как-то: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных устройств, генераторы измерительных приборов и т.д.

При внешних воздействиях информационного сигнала (например, электромагнитных полей) на элементах ВЧ генераторов индуктируются электрические сигналы. Приемными антеннами для магнитного поля могут служить катушки индуктивности колебательных контуров, сглаживающие дроссели в цепях электропитания и т.д. Приемниками электрического поля являются провода высокочастотных цепей и другие элементы. Индуктированные электрические сигналы могут вызвать модуляцию собственных ВЧ колебаний генераторов и излучение их в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные в результате фазового сдвига сигнала обратной связи на определенных частотах, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.), переходящих в нелинейный режим работы при перегрузке за счет действия положительной обратной связи. Сигнал на

частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны.

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

1.2.2. Электрические каналы утечки информации

Электрические каналы утечки информации образуются за счет:

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

1.2.2.1. Наводки электромагнитных излучений ТСПИ

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

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

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

Случайные антенны могут быть сосредоточенными и распределенными. *Сосредоточенная случайная антенна* представляет собой техническое средство небольшого объема, например телефонный аппарат, громкоговоритель радиотрансляционной сети, реле и т.д. К *распределенным случайным антеннам* относятся случайные антенны с распределенными параметрами (длинные линии): кабели, провода, металлические трубы и другие токопроводящие устройства.

Просачивание информационных сигналов в цепи электропитания. Просачивание возможно при наличии взаимоиндуктивной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Наводки на вторичные источники питания (ВИП), можно разделить на три вида: наводки в виде переменного напряжения с частотой питающей сети или ее гармоник, высокочастотные наводки, появляющиеся вследствие антенного эффекта проводов питающей сети, наводки, возникающие внутри блока вследствие появления паразитных связей через общие провода питания различных элементов.

Основными причинами появления помехи с частотой питающей сети или ее гармоник являются недостаточное сглаживание пульсаций в ВИП, паразитные связи элементов с первичными цепями ВИП, неэквипотенциальность точек заземления, наличие общих проводов питания, по которым возможна гальваническая связь. Из всех причин только первая не является следствием паразитных процессов. Величина наводки зависит не только от вида паразитной связи, но и от схемы подключения двухфазных ВИП к трехфазной промышленной сети.

В канале связи при емкостной паразитной связи (рис. 1.13) для схемы питания без нулевого провода помеха будет [3]

$$U_{\text{п.п}} = (U_1 C_{\text{п}1} - U_2 C_{\text{п}2}) R_{\text{к}} \omega_{\text{п}} / \sqrt{1 + T_{\text{к}}^2 \omega_{\text{п}}^2}, \qquad (1.41)$$

где $C_{\text{п}1}, C_{\text{п}2}$ – паразитные емкости канала связи с фазными проводами, в общем случае $C_{\text{п}1} \neq C_{\text{п}2}$; $\omega_{\text{п}}$ – частота питающей сети; $R_{\text{к}}, T_{\text{к}}$ – внутреннее сопротивление и постоянная времени канала связи.

Из (1.41) видно, что для снижения наводки необходимо добиваться равенства $C_{\text{п}1} = C_{\text{п}2}$ и $U_1 = U_2$.

Для выполнения равенства $C_{\text{п}1} = C_{\text{п}2}$ необходимо подводку переменных напряжений выполнять симметричной двухпроводной линией с минимально возможным расстоянием между проводами, чаще всего для этого используют витую пару. Выполнение равенства $U_1 = U_2$ не зависит от потребителя и в общем случае не обеспечивается.

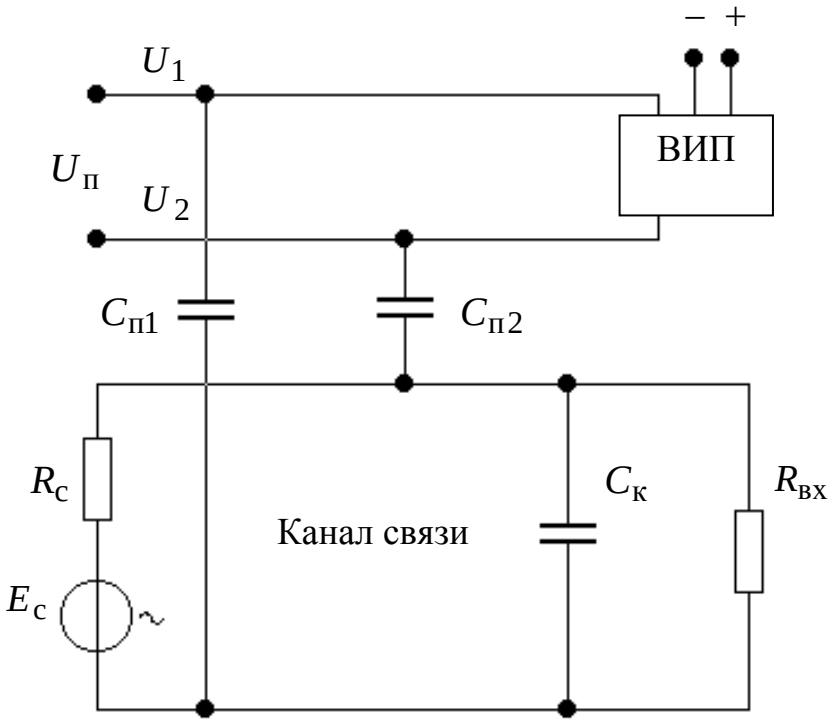


Рис. 1.13. Схема емкостной внешней паразитной связи с первичной цепью ВИП

Помехи в схеме с нулевым проводом можно рассчитать по (1.41), подставив U_0 вместо U_2. В этом случае для снижения наводки имеется только один путь – снижение паразитной емкости $C_{п1}$.

Вторая причина появления наводки с частотой питающей сети заключается в наличии общих проводов.

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

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

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

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

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

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

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют *телефонными закладками.*

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных элек-

трических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

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

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

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

1.2.3. Параметрический канал утечки информации

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

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

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

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

1.3. Технические каналы утечки информации при передаче ее по каналам связи

Для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи.

1.3.1. Электрические линии связи

1.3.1.1. Средства передачи электрических сигналов

Работа любого электронного устройства основана на получении, обработке и передаче информации, представленной в виде электрических сигналов. В передаче электрического сигнала участвуют источник, средства передачи и приемник сигнала. Устройства передачи электрических сигналов от источника к приемнику называют *электромагнитными линиями связи* или кратко – *линиями связи* [3]. Линии связи используют в качестве средства передачи энергию электрического поля, магнитного поля, электромагнитного поля излучения, электрические проводники и волноводы.

Напряженность электрического и магнитного полей в пространстве убывает обратно пропорционально квадрату расстояния от элемента, являющегося источником поля. Минимальные потери энергии характерны для однородного электрического поля, локализованного в определенной области пространства, например, в электрических конденсаторах.

Для создания магнитных полей применяют катушки индуктивности с ферромагнитными сердечниками или без них. Наличие ферромагнитного сердечника способствует локализации магнитного поля в пределах сердечника и снижению потерь энергии. В катушках без сердечника пространство распространения магнитного поля ненамного больше. В электронных устройствах конденсаторы и катушки индуктивности используют как средства для формирования требуемых частотных и фазовых характеристик линий связи.

Полная независимость между электрическим и магнитным полями может иметь место только в статических режимах. При упорядоченном перемещении электрических зарядов возникает электрический ток и, как следствие, магнитное поле. С другой стороны, при любом перемещении проводника в магнитном поле появляется ЭДС, что сопровождается появлением электрического поля. Таким образом, электрическое и магнитное поля неразрывно связаны и являются составляющими электромагнитного поля. Любое изменение магнитного поля сопровождается индукцией ЭДС, изменяющую вектор электрического поля. Отсутствие полной независимости электрического и магнитного полей принципиально не позволяет создать идеальные конденсаторы, не обладающие паразитной индуктивно-

стью, и идеальные катушки индуктивности, не имеющие собственной паразитной емкости.

Симметричные двухпроводные линии связи (рис. 1.14) имеют два провода, по одному из которых течет прямой ток, а по другому – обратный. Симметричные двухпроводные линии могут быть реализованы в виде двух параллельных проводов, закрепленных на изолирующих распорках (рис. 1.14, *а*), или иметь непрерывную гибкую оболочку (рис. 1.14, *б*) из диэлектрика, или в виде двух свитых проводов (рис. 1.14, *в*), или в виде двух одинаковых печатных проводников, расположенных с одной (рис. 1.14, *г*) или с двух (рис. 1.14, *д*) сторон печатной платы.

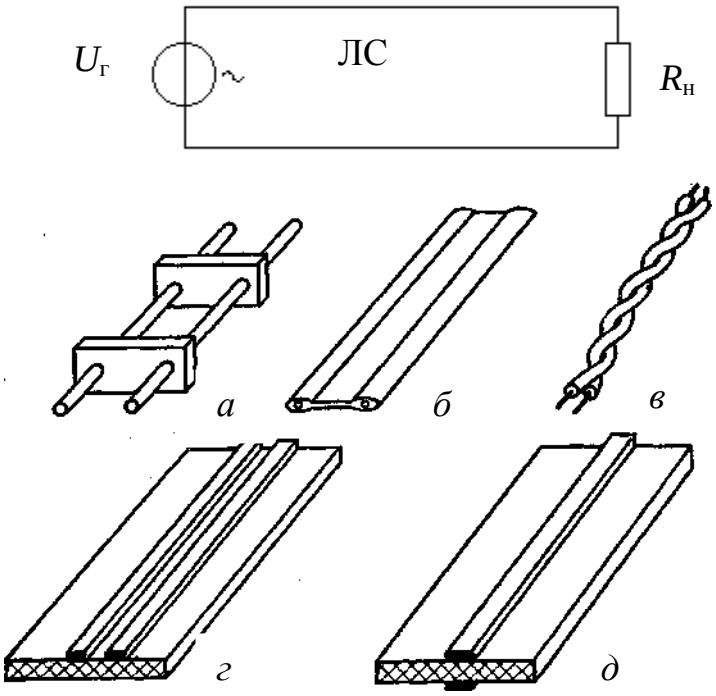


Рис. 1.14. Электрическая схема и варианты конструктивного исполнения двухпроводных симметричных линий связи:
а – жесткая линия на распорках; *б* – гибкая ленточная линия; *в* – витая пара; *г* – односторонняя печатная линия; *д* – двусторонняя печатная линия; $U_г$ – напряжение генератора; $R_н$ – сопротивление нагрузки

Линии связи (ЛС), выполненные на печатной плате, называют полосковыми. Несимметричные однопроводные линии связи (рис. 1.15) состоят из одного провода, по которому проходит прямой ток. В качестве обратного провода могут использоваться корпус блока, земляная шина, шина питания или провод, общий для нескольких линий связи. Несимметричные однопроводные линии могут быть реализованы в виде одиночного объемного (рис. 1.15, *а*) или печатного (рис. 1.15, *б–г*) проводников. В несимметричных однопроводных ЛС токи, текущие по прямому и обратному проводам, в общем случае не равны между собой.

Коаксиальный кабель, представляющий собой экранированный провод, состоит из двух цилиндрических проводов, вставленных концентрично один в другой (рис. 1.16, *а*). Прямой ток проходит по центральному проводу, обратный – по оболочке (рис. 1.16, *б*).

Линии связи обладают электрическими и конструктивными параметрами. Электрические параметры ЛС подразделяются на первичные и вторичные [3].

К первичным параметрам относятся $L_{\text{п}}$ – погонная индуктивность, $C_{\text{п}}$ – погонная емкость, $R_{\text{п}}$ – погонное сопротивление потерь, $G_{\text{п}}$ – погонная проводимость линии.

К вторичным параметрам относятся $Z_{\text{в}}$ – волновое сопротивление, $K_{\text{в}}$ – коэффициент укорочения волны в линии.

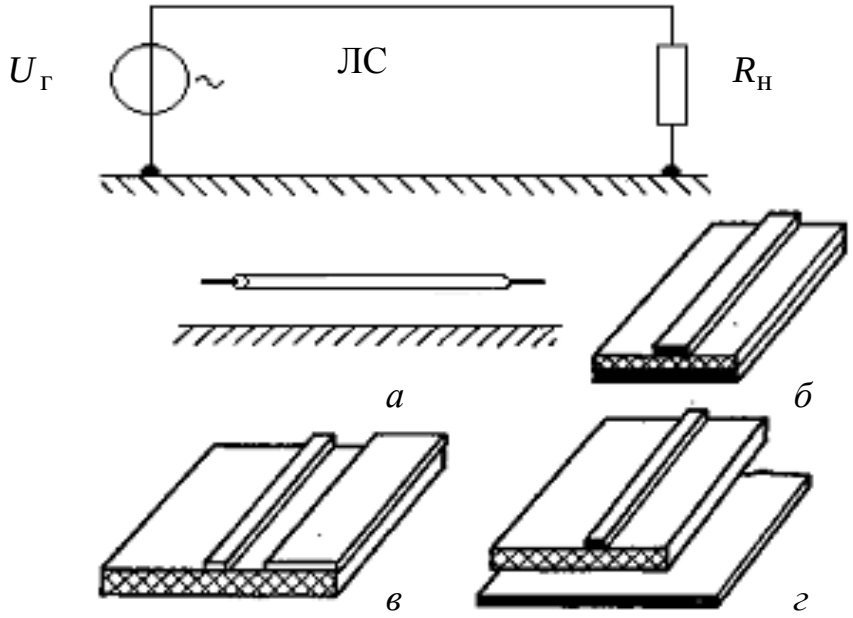


Рис. 1.15. Электрическая схема и варианты конструктивного исполнения несимметричных однопроводных линий связи:
а – объемный проводник; *б* – печатный проводник на двусторонней плате;
в – печатный проводник на односторонней плате с общим проводом на плате;
г – печатный проводник вблизи токопроводящего корпуса (общего провода)

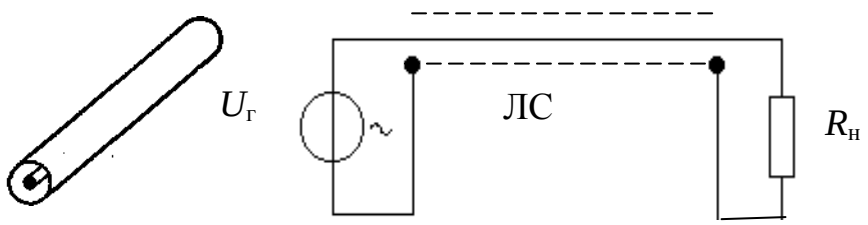
Конструктивные параметры составляют длина линии $l_{\text{с}}$, форма и размеры проводников, расстояние между проводниками, электромагнитные свойства материала проводников и окружающей среды.

Вторичные параметры линии определяются через первичные и конструктивные параметры:

$$Z_{\text{вт}} = \sqrt{(R_{\text{п}} + j\omega L_{\text{п}})/(G_{\text{п}} + j\omega C_{\text{п}})};$$

$$K_{\text{в}} = V_0 / V_{\text{с}},$$

где ω – частота сигнала, передаваемого линией связи; $V_0 = 1/\sqrt{\mu_0 \varepsilon_0}$ – скорость распространения электромагнитной волны в открытом пространстве (скорость света); $V_c = 1/\sqrt{\mu_0 \varepsilon_0 \mu \varepsilon}$ – скорость распространения электромагнитной волны в линии связи; $\mu_0 = 4\pi \cdot 10^{-7}$ – абсолютная магнитная проницаемость вакуума, Гн/м; $\varepsilon_0 = 1/(36\pi \cdot 10^9)$ – абсолютная диэлектрическая постоянная вакуума; μ, ε – относительные магнитная и диэлектрическая постоянные среды, в которой расположены проводники линии.



а *б*

Рис. 1.16. Коаксиальная линия связи (*а*) и электрическая схема ее включения (*б*)

Электромонтажные линии связи в микроэлектронных устройствах могут иметь вид системы проводников круглого сечения в объемном монтажном пространстве, или вид плоских проводников на печатной плате.

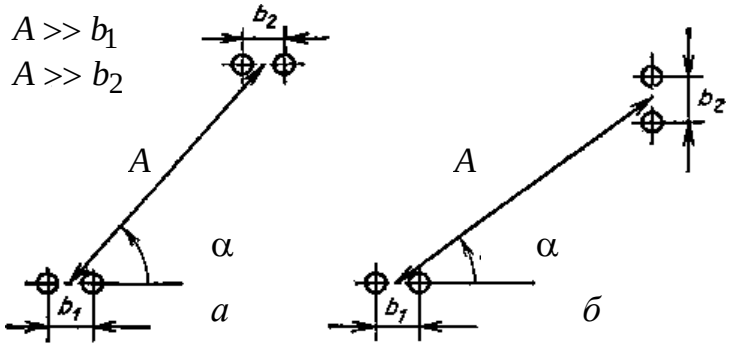


Рис. 1.17. Линии связи, лежащие в параллельных (*а*) и взаимно перпендикулярных плоскостях (*б*)

Взаимная индуктивность двух электромонтажных ЛС зависит от взаимного расположения и расстояния между проводами линий. Для двух линий, лежащих в параллельных плоскостях (рис. 1.17, *а*), взаимная индуктивность

$$M = (\mu\mu_0 l b_1 b_2 \cos 2\alpha)/(\pi A^2); \qquad (1.42)$$

для линий, лежащих во взаимно перпендикулярных плоскостях (рис. 1.17, *б*),

$$M = (\mu\mu_0 l b_1 b_2 \sin 2\alpha)/(\pi A^2). \qquad (1.43)$$

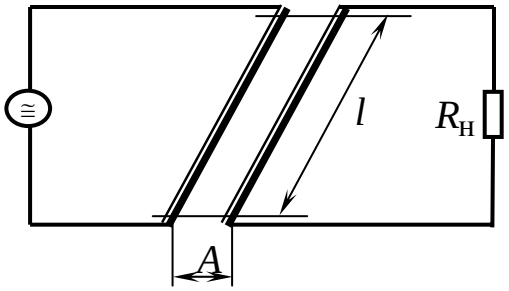


Рис. 1.18. К расчету взаимной индуктивности двух одиночных проводов

Взаимная индуктивность двух одиночных проводов (рис. 1.18) определяется выражением

$$M = \frac{\mu\mu_0}{2\pi} l \ln\left(\frac{2l}{A} - 1\right). \qquad (1.44)$$

1.3.2. Каналы утечки информации за счет паразитных связей

1.3.2.1. Опасные сигналы и их источники

Утечка информативного сигнала по цепям электропитания и слаботочных линий может происходить различными путями. Например, между двумя электрическими цепями, находящимися на некотором расстоянии друг от друга, могут возникнуть электромагнитные связи, создающие объективные предпосылки для появления информативного сигнала в цепях системы электропитания объектов вычислительной техники (ВТ). Эти процессы называются наводками, которые обеспечивают передачу энергии из одного устройства в другое, не предусмотренную схемными или конструктивными решениями.

Источниками наводки являются устройства, в которых обрабатывается информативный сигнал; приемниками – цепи электропитания, выступающие в качестве токопроводящей среды, выходящей за пределы контролируемой территории и одновременно с этим представляющие собой опасный канал утечки информации, обрабатываемой ПЭВМ и ЛВС.

Утечка информации при функционировании средств ВТ также возможна либо через непосредственное излучение и наведение информативных импульсов, циркулирующих между функционально законченными узлами и блоками, либо посредством высокочастотных электромагнитных сигналов, модулированных информативными импульсами и обладающих способностью самонаводиться на провода и общие шины электропитания через паразитные связи.

Объекты, излучающие сигналы, содержат источники сигнала. Если объект отражает поля внешних источников, то он является источником информации об объекте и в то же время является источником сигнала.

Может быть такой источник сигнала, который переписывает информацию с одного носителя на другой. Если источником сигнала является радиозакладка и первичным – речевой сигнал от говорящего человека. Мембрана является преобразователем акустического сигнала в электрический. Такой источник сигнала называется передатчиком.

Если источник сигнала применяется для обеспечения связи между санкционированными объектами, то такие источники называются функциональными источниками сигнала. Существуют источники опасных сигналов – это источники от которых могут распространяться несанкционированным образом сигналы защищаемой информации.

Источником сигналов могут быть любые объекты излучения.

Источниками опасных сигналов могут быть:

1) акустоэлектрические преобразователи (пьезоэлектрические, емкостные, индуктивные);

2) излучатели низкочастотных сигналов (элементы РЭС, усилительные каскады, генераторы, ПЭВМ);

3) излучатели высокочастотных сигналов;

4) паразитные связи и наводки (гальванические, индуктивные, емкостные).

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

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

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

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

Внешняя параллельная емкостная паразитная связь. В электронных устройствах чаще других имеет место внешняя параллельная емкостная паразитная связь [3]. Эквивалентная схема паразитной емкостной связи представлена на рис. 1.19. Сопротивление $Z_{вх1}$ представлено в виде параллельно соединенных $R_{вх1}$ и $C_{вх1}$, что правомерно для большинства устройств, работающих на низких

и средних частотах. Второй канал показан упрощенно, так как его параметры слабо влияют на значение наводки из второго канала в первый.

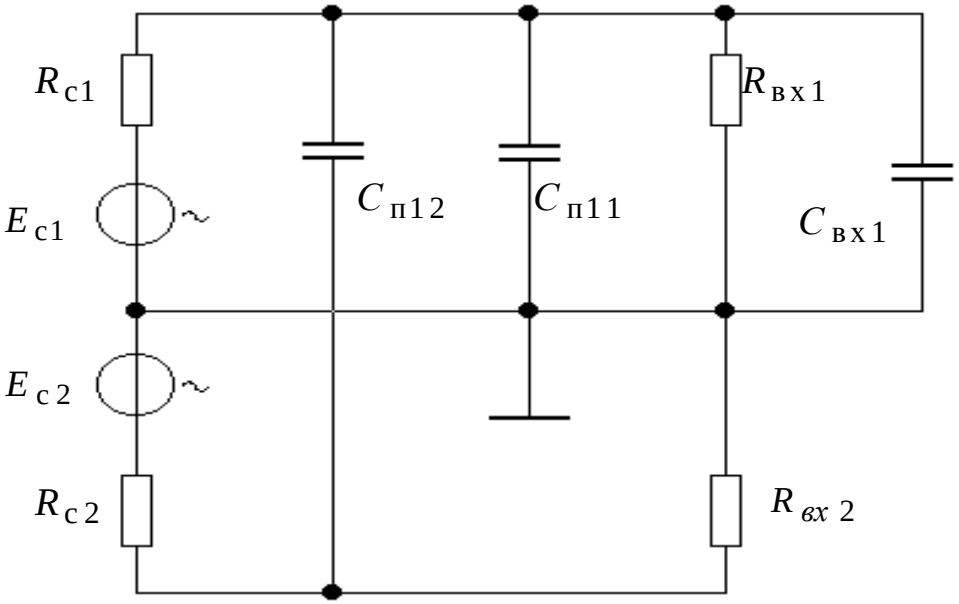


Рис. 1.19. Эквивалентная схема внешней емкостной параллельной паразитной связи между двумя каналами

Рассмотрим расчет помехи $U_{п.п12}$, наводимой из второго канала в первый. Напряжение сигнала во втором канале (на сопротивлении $R_{вх2}$) определяется выражением

$$U_{с2} = E_{с2} R_{вх2} / (R_{с2} + R_{вх2}). \qquad (1.45)$$

Входное сопротивление первого канала связи для сигнала наводки образуется параллельным соединением следующих элементов: выходного сопротивления генератора $R_{с1}$, паразитной емкости линии связи $C_{п11}$, входного сопротивления приемника сигнала $R_{вх}$ и входной емкости приемника сигнала, т. е.

$$Z_{к1} = X_{с1} R_{к1},$$

где $X_{с1}$ – импеданс паразитной емкости $C_{п11}$;

$$C_{к1} = C_{п11} + C_{вх1} + C_{п12}; \;\; R_{к1} = R_{вх1} R_{с1} / (R_{вх1} + R_{с1}),$$

$R_{к1}, C_{к1}$ – входное сопротивление и собственная емкость первого канала.

$$U_{п.п12} = U_{с2} T_{п12} \omega_{с2} / \sqrt{1 + T_{к1}^2 \omega_{с2}^2}, \qquad (1.46)$$

где $T_{к1} = R_{к1} C_{к1}$ – постоянная времени первого канала связи; $T_{п12} = R_{к1} C_{п12}$ – постоянная времени цепи паразитной связи первого канала со вторым; $\omega_{с2}$ – частота гармонического сигнала во втором канале.

Передаточная функция канала емкостной параллельной паразитной связи

$$W_{\text{п.п12}}(p) = pC_{\text{п12}}R_{\text{к1}}/(pR_{\text{к1}}C_{\text{к1}}+1) = T_{\text{п12}}p/(T_{\text{к1}}p+1), \qquad (1.47)$$

а в соответствии с передаточной функцией определяется амплитудно-частотная характеристика

$$A_{\text{п.п12}}(\omega) = T_{\text{п12}}\omega_{c2}/\sqrt{1+T_{\text{к1}}{}^2\omega_{c2}^2}, \qquad (1.48)$$

где ω_{c2} – частота гармонического сигнала во втором канале.

Паразитные связи последовательного вида. Появление паразитных связей последовательного вида возможно при наличии общих проводов и не равных нулю значений выходных сопротивлений вторичных источников питания, шин питания, земляных цепей.

Причиной появления последовательной помехи (наводки) на высоких частотах является паразитная связь из-за взаимной индуктивности между проводами (рис. 1.20). В этом случае отсутствие общих проводов не гарантирует отсутствие токовой наводки.

При гармоническом сигнале токовая наводка

$$U_{\text{т.п12}} = E_{\text{с2}}\omega_{\text{с2}}M_{\text{п12}}/(R_{\text{вх2}}+R_{\text{с2}}). \qquad (1.49)$$

В случае импульсных сигналов величина токовой наводки в первом канале связи определяется крутизной фронтов $t_{\text{ф}}$ импульса во втором канале:

$$U_{\text{т.п12}} = M_{\text{п12}}\frac{di_2}{dt} = \frac{E_{c2}}{t_{\text{ф}}}\cdot\frac{M_{\text{п12}}}{R_{c2}+R_{\text{вх2}}}. \qquad (1.50)$$

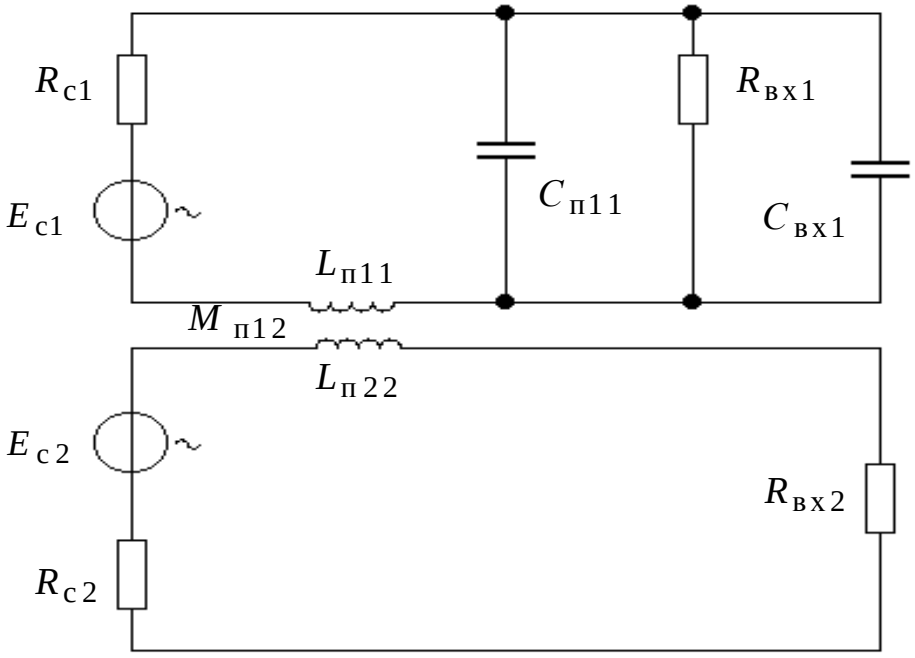


Рис. 1.20. Эквивалентная схема последовательной паразитной связи через паразитную взаимную индуктивность

Паразитные связи через посторонний провод. Пусть между двумя устройствами, размещенными в двух отдельных экранированных блоках и образующими две линии связи – первую и вторую, проходит третий провод, не относящийся к линиям связи 1 и 2, т. е. являющийся посторонним для линий связи 1 и 2, но имеющий с ними паразитные емкости $C_{п13}$ и $C_{п23}$ (рис. 1.21) или паразитные взаимоиндуктивности $M_{п13}$ и $M_{п23}$ (рис. 1.22).

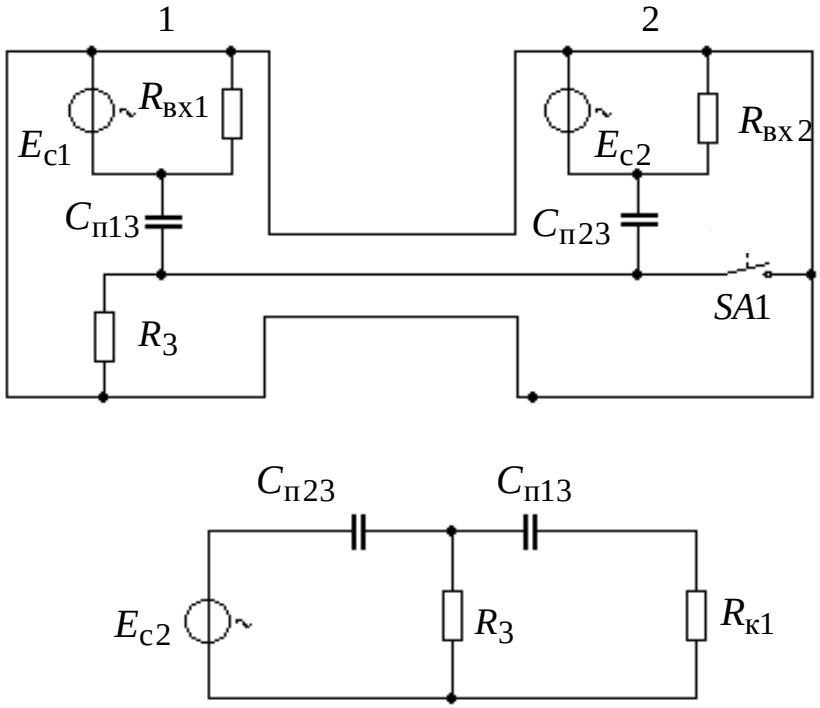


Рис. 1. 21. Индуктивная связь через посторонний провод
и ее эквивалентная схема

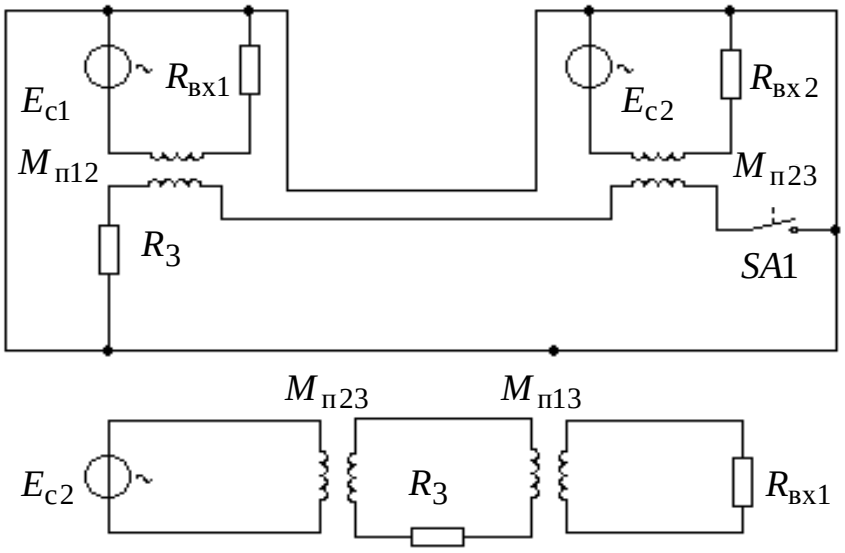


Рис. 1. 22. Индуктивная связь через посторонний провод и ее эквивалентная схема

Значение наводки можно рассчитать по формулам (1.46)–(1.49), считая третий провод приемником наводки по отношению к каналу связи 2 и источником наводки по отношению к каналу 1. Анализ показывает, что в случае емкостной паразитной внешней связи через посторонний провод уменьшение величины собственного сопротивления R_3 постороннего провода снижает наводки, при индуктивной паразитной связи снижение сопротивления R_3 увеличивает сигнал наводки. Если в схеме на рис. 1.21 замкнуть ключ SA1, то наводка исчезнет.

В схеме на рис. 1.22 наводка возможна только при замкнутом ключе SA1, так как только в этом случае возникает потокосцепление постороннего провода. В сложных системах не всегда возможно определить посторонний провод, создающий паразитную связь.

1.3.3. Электрические каналы утечки информации

Электрический канал утечки информации при ее передаче по линиям связи может быть образован путем непосредсвенного контактного подключения к кабельным линиям аппаратуры перехвата. Для повышения скрытности аппаратура перехвата подключается к линии через специальные согласующие устройства, снижающие вносимое сопротивление и падение напряжения на линии. Некоторые кабели связи для защиты от подключения устройств перехвата снабжаются воздухонепроницаемой оболочкой, внутри которой поддерживается избыточное контролируемое давления воздуха. В этом случае средства перехвата должны иметь возможность компенсации снижения давления воздуха при подключении к кабелю.

Этот канал наиболее часто используется для перехвата низкочастотных телефонных сигналов в линиях связи в местах свободного доступа. В дальнейшем перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Если подобные устройства содержат радиопередатчики для ретрансляции перехваченной информации, то их называют телефонными закладками.

1.3.3.1. Контроль и прослушивание телефонных каналов связи

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

- Параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы (телефонные закладки) труднее обнаруживаются, но требуют внешнего источника питания.
- Последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. В этом случае питание телефонного

радиоретранслятора осуществляется от телефонной линии и на передачу он выходит с момента подъема телефонной трубки абонементом.

Подключение телефонного радиоретранслятора может осуществляться как непосредственно к телефонному аппарату, так и к любому участку линии от телефона абонента до АТС. В настоящее время существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение через микрофон лежащей трубки. Для этого на один провод телефонной линии подключается генератор высокочастотных колебаний, а к другому – амплитудный детектор с усилителем. Высокочастотные колебания проходят через микрофон или элементы телефонного аппарата, обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения. Модулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления прослушивается или записывается.

Дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает нескольких десятков метров. Имеются системы прослушивания телефонных разговоров, которые не требуют непосредственного электронного соединения с телефонной линией. Эти системы основаны на индуктивном способе съема информации при помощи специальных катушек. Они сложны и громоздки, поскольку содержат несколько каскадов усиления слабого низкочастотного сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого практического применения.

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

Непосредственное подключение к телефонной линии. Непосредственное подключение к телефонной линии – наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаще всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб).

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

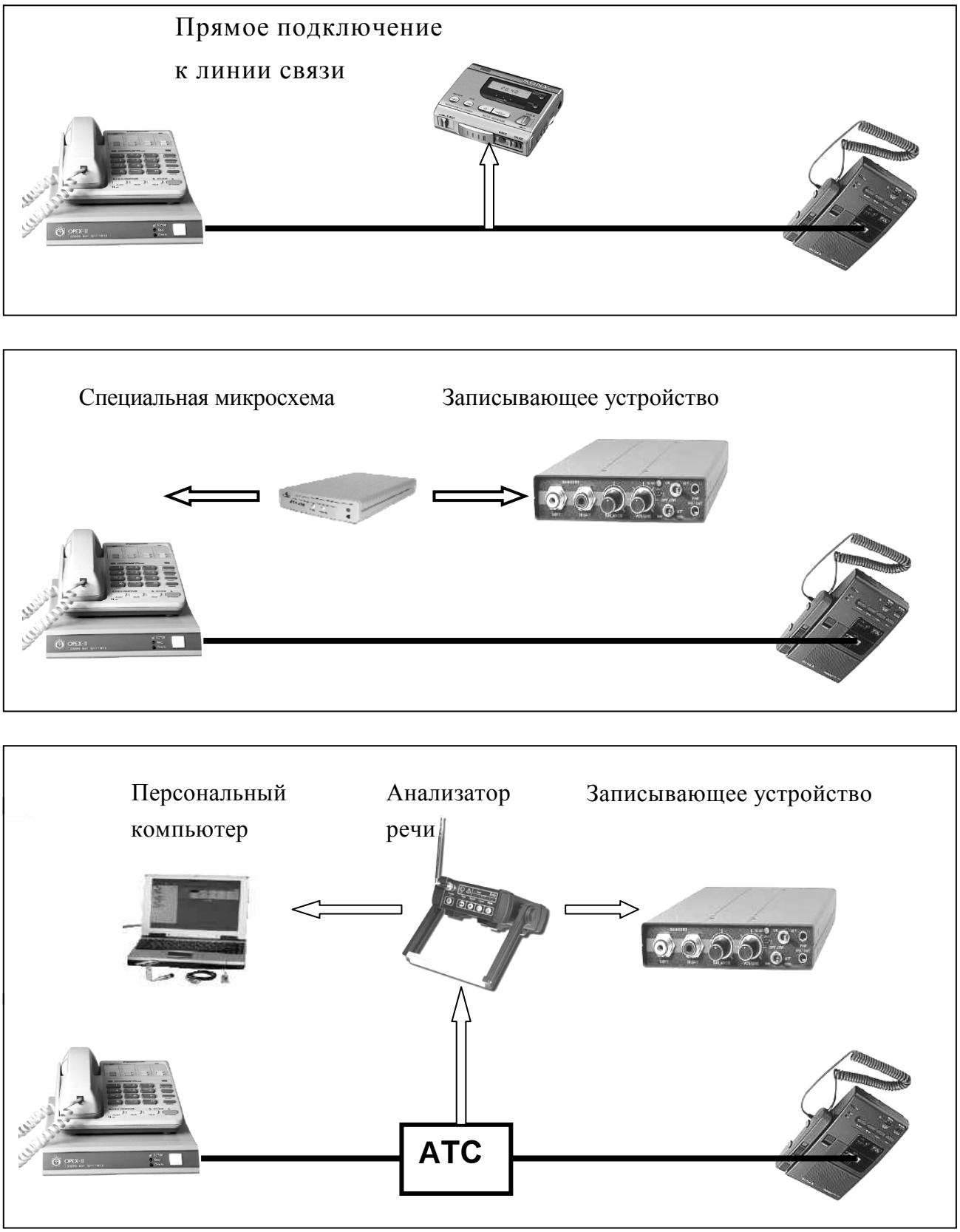


Рис. 1.23. Схемы возможных вариантов подключения к телефонной линии без использования радиоканала

Рис. 1.24. Схемы возможных вариантов подключения к телефонной линии с использованием радиоканала

На рис. 1.25 приведена схема прослушивания помещения способом, называемым высокочастотным навязыванием. Этот способ аналогичен способу высокочастотной накачки и состоит в следующем.

На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора Г. К другому проводу линии подключается детектор, выполненный на элементах Cl, C2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и при-

емника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

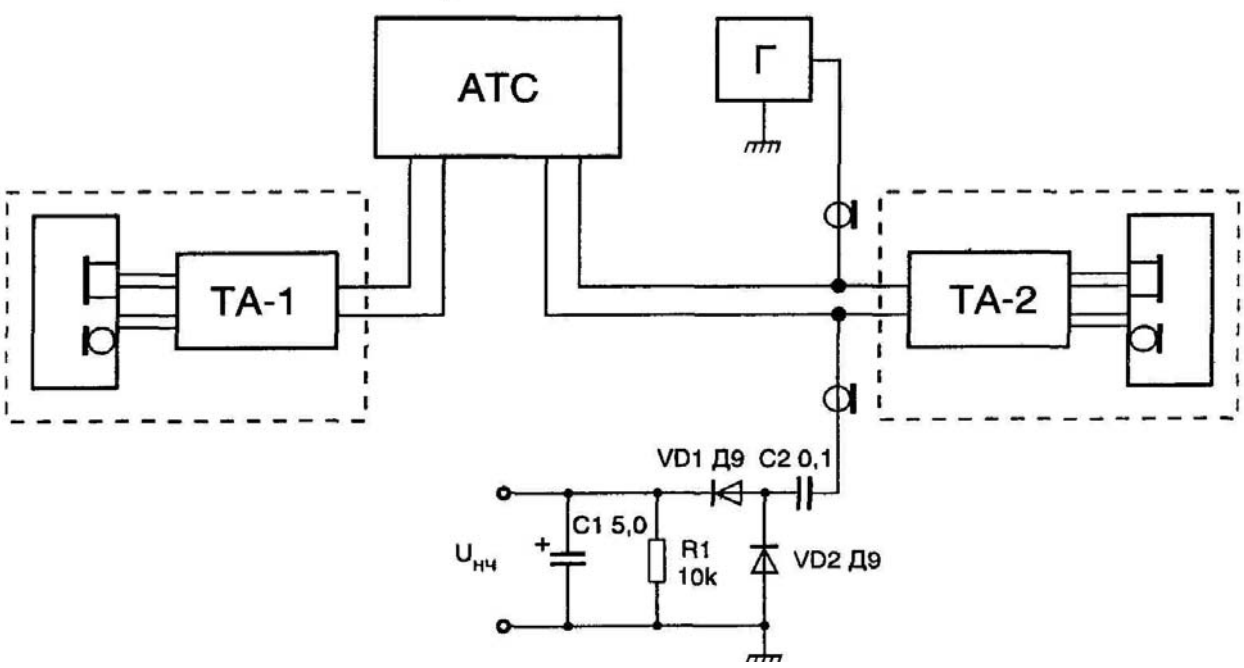


Рис. 1.25. Прослушивание через микрофон телефонного аппарата

Недостаток этого метода состоит в том, что его случайно может обнаружить всякий, кто позвонит по тому же номеру, а также необъяснимая занятость контролируемой линии для других абонентов.

1.3.4. Электромагнитные каналы утечки информации

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться с использованием стандартных технических средств радиоразведки. Этот электромагнитный канал перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

1.3.5. Индукционный канал утечки информации

Данный канал чаще всего используется для съема информации с симметричных высокочастотных кабелей. Непосредственное электрическое подключение аппаратуры перехвата легко обнаруживается специальными контролирующими средствами. Индукционный канал перехвата, не требующий контактного подключения к каналам связи, свободен от этого недостатка. Электромагнитное поле, возникающее вокруг проводников кабеля под действием информационных токовых сигналов, наводит в специальных индукционных датчиках адекватные информационные сигналы.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

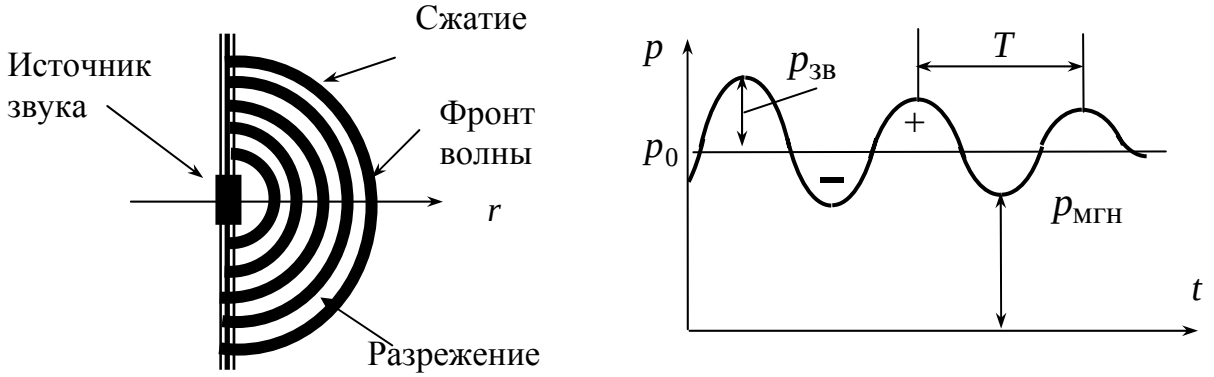
1.4. Технические каналы утечки речевой информации

1.4.1. Краткие сведения по акустике

1.4.1.1. Звуковое поле

Звуковое поле представляет собой пространство, в котором распространяются звуковые колебания. Звуковые колебания в газообразной и жидкой средах являются продольными, так как частицы вещества среды колеблются вдоль линии распространения звука r (рис. 1.26, *а*). Под воздействием источника звука, например, гармонического характера, образуются сжатия и разрежения среды, которые перемещаются от источника со скоростью звука. *Скорость звука* в воздушной среде при нормальном атмосферном давлении и температуре 20 °С примерно равна $c_{зв} \approx 340$ м/с.

Волнообразное изменение плотности p среды (рис. 1.26, *б*), обусловленное звуковыми колебаниями, называют *звуковым лучом*, а поверхность с одинаковыми фазами колебаний – *фронтом волны*. Фронт волны перпендикулярен звуковому лучу.



а *б*

Рис. 1.26. Звуковые колебания (*а*) и изменение звукового давления в фиксированной точке звукового поля (*б*)

Частота колебаний $f = 1/T$ определяется периодом колебаний, а длина звуковой волны $\lambda = cT$. Частоты звуковых колебаний находятся в полосе частот от 20 до 20000 Гц. Не воспринимаемые органом слуха частоты ниже 20 Гц называют инфразвуковыми, а выше 20000 Гц – ультразвуковыми. В системах связи длины звуковых волн находятся в пределах от 17–11,3 м до 2,27–1,7 см.

Частоты колебаний подразделяются на низкие, средние и высокие звуковые частоты. К низким относятся частоты в диапазоне от 20 до 500 Гц, к средним – от 500 до 2000 Гц, к высоким – от 2000 до 20000 Гц.

Звуковое поле характеризуется некоторыми линейными и энергетическими величинами.

1.4.1.2. Линейные характеристики звукового поля

Звуковое давление. Давление среды p_0 при отсутствии звуковых колебаний называют статическим (рис. 1.26, *б*). При распространении звуковой волны давление в определенной точке среды непрерывно изменяется: при сгущении частиц оно увеличивается до уровня, превышающего статическое давление, а при разряжении становится ниже уровня статического давления. Звуковым давлением называют разность между мгновенным значением давления в определенной точке пространства и статическим давлением:

$$p_{\text{зв}}(t) = p_{\text{мгн}}(t) - p_0.$$

Звуковое давление является знакопеременной величиной и определяется как сила, действующая на единицу площади:

$$p_{\text{зв}}(t) = F/S \ \ [\text{Н}/\text{м}^2].$$

Скорость колебаний. При не одинаковых давлениях в рядом расположенных точках среды ее частицы перемещаются в сторону меньшего давления. При знакопеременной разности давлений возникает колебательное движение частиц относительно статического положения. Если обозначить через *u* смещение частиц, то скорость колебаний определяется как первая производная по времени от смещения $v = du/dt$ [м/с]. Скорость колебаний в отличие от скорости звука величина переменная. Если частицы среды смещаются по направлению распространения волны, то скорость считают положительной.

Если смещение частиц среды подчиняется гармоническому закону $r = r_m e^{j\omega t}$ с угловой частотой $\omega = 2\pi f$, то колебательная скорость $v = \dfrac{dr}{dt}$ в комплексной форме запишется как $j\omega r_m e^{j\omega t}$. За время одного периода колебаний фронт звуковой волны перемещается на расстояние, равное длине волны λ.

Для определения связи звукового давления с колебательной скоростью рассмотрим элементарный слой воздуха, расположенный между фронтами волн и имеющий толщину Δr [37] (рис. 1.27). Фронтальные плоскости, расположенные перпендикулярно звуковым лучам *r*, имеют площадь ΔS. Среда в выделенном объеме находится под воздействием разности давле-

ний $p_{зв}$ и $p_{зв}+\Delta p_{зв}$, в результате чего на среду действует сила $\Delta F=[p_{зв}-(p_{зв}+\Delta p_{зв})]\Delta S=-\Delta p_{зв}\Delta S$. С другой стороны, сила инерции $\Delta F=\Delta m\dfrac{dv}{dt}=\rho\Delta r\Delta S\dfrac{dv}{dt}$, где Δm – масса среды элементарного объема, ρ – средняя плотность среды. Приравнивая силы из двух последних уравнений, получим $\Delta p_{зв}=-\rho\Delta r\dfrac{dv}{dt}$.

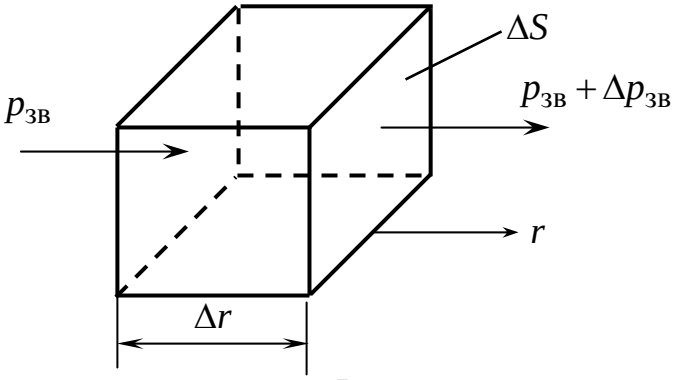


Рис. 1.27

Так как $p_{зв}$ и v зависят и от координат и от времени, то при переходе к частным производным получаем уравнение движения среды

$$-\frac{\partial p_{зв}}{\partial r}=\rho\frac{\partial v}{\partial t}. \qquad (1.51)$$

1.4.1.3. Энергетические характеристики звукового поля

Звуковая мощность представляет собой скорость изменения работы звуковой волны A в направлении распространения звуковых волн через всю площадь фронта волны. Физически работа обусловлена сопротивлением среды распространению звуковых волн. Звуковая мощность определяется выражением

$$P=dA/dt=F\,dr/dt=Fv=p_{зв}Sv \ \text{[Вт]}. \qquad (1.52)$$

Интенсивность (сила) звука – это поток звуковой энергии, проходящий в единицу времени через единицу поверхности фронта волны. Согласно определению мгновенное значение акустической мощности равно произведению мгновенных значений силы F и скорости колебаний v: $P=Fv$.

Удельная мощность звуковых колебаний. Удельная мощность колебаний определяется как

$$P_{уд}=p_{зв}v=Fv/S=P/S=I \ \text{[Вт/м}^2\text{]} \qquad (1.53)$$

и называется силой звука.

Плотность звуковой энергии ε представляет собой среднее значение звуковой энергии в единице объема среды. Свяжем понятия интенсивности

звука и плотности энергии. Для этого выделим объем среды по направлению распространения волны (рис. 1.27). Энергия в объеме среды ΔV в рассматриваемый момент времени $\Delta W = \varepsilon \Delta V = \varepsilon \Delta r \Delta S$ уйдет из него за время $\Delta t = \Delta r / c_{зв}$, где $c_{зв}$ – скорость звука. Поток энергии $\Delta W / \Delta t = c_{зв} \varepsilon \Delta r \Delta S / \Delta r = c_{зв} \varepsilon \Delta S$. Подставив данное выражение в формулу $I = \Delta W / \Delta S \Delta t$ и выполнив соответствующие преобразования, определим плотность звуковой энергии

$$\varepsilon = I / c_{зв}. \qquad (1.54)$$

1.4.1.4. Плоская волна

Плоская волна является случаем направленного излучения звука источником, когда звуковые лучи параллельны друг другу и перпендикулярны направлению распространения. Параллельность лучей указывает на не расходящийся характер энергии в пространстве. При этом фазы звуковых колебаний будут одинаковы в перпендикулярных направлению распространения звуковых волн сечениях. Плоская волна возникает в тех случаях, когда размеры звуковых излучателей больше длины волны. В идеальном случае (при отсутствии вязкости среды) интенсивность звука не должна была бы уменьшаться, но реально потери существуют. В расчетах для небольших расстояний обычно этими потерями пренебрегают.

Пусть источник излучает плоскую волну гармонической формы $p_{зв} = p_{зв.m} e^{j\omega t}$ с нулевой начальной фазой [37]. На некотором удалении r от источника давление вследствие инерционности среды будет запаздывать по фазе на время $\tau = r / c_{зв}$ и примет значение

$$p_{зв} = p_{зв.m} e^{j\omega(t-\tau)}. \qquad (1.55)$$

Введем понятие волнового числа $k = \omega / c = 2\pi / \lambda$, которое определяет коэффициент изменения фазы на единицу расстояния, а выражение (1.55) представим в форме $p_{зв} = p_{зв.m} e^{j(\omega t - \omega\tau)}$. С учетом того, что $c_{зв} = \frac{\omega}{k}$, а $\omega\tau = \frac{\omega r}{c} = \frac{\omega r k}{\omega} = kr$, выражение (1.55) принимает более удобную форму

$$p_{зв} = p_{зв.m} e^{j(\omega t - kr)}. \qquad (1.56)$$

Как следует из ранее полученного выражения (1.51) $-\frac{\partial p_{зв}}{\partial r} = \rho \frac{\partial v}{\partial t}$, а первая производная по времени от колебательной скорости $\frac{\partial v}{\partial t} = -\frac{1}{\rho} \frac{\partial p_{зв}}{\partial r}$, откуда с учетом (1.56) определим

$$v = j\frac{k\,p_{\text{зв}.m}}{\rho}\int e^{j(\omega t - kr)}dt = \frac{k\,p_{\text{зв}.m}}{\rho\omega}e^{j(\omega t - kr)}. \qquad (1.57)$$

Сравнение выражений (1.56) и (1.57) показывает, что звуковое давление и колебательная скорость в плоской волне не имеют сдвига по фазе.

Если учесть, что $p_{\text{зв}} = p_{\text{зв}.m}e^{j(\omega t - kr)}$ и $c_{\text{зв}} = \frac{\omega}{k}$, то выражение (1.57) можно представить как

$$v = \frac{p_{\text{зв}}}{\rho c_{\text{зв}}} = \frac{p_{\text{зв}}}{z_{\text{а}}}, \qquad (1.58)$$

где $z_{\text{а}} = \rho c_{зв}$ называют удельным акустическим сопротивлением.

Произведение удельного акустического сопротивления на всю площадь поверхности акустического излучателя составляет полное сопротивление среды (сопротивление излучения):

$$z_R = z_{\text{а}}S = \rho c_{\text{зв}}S = p_{\text{зв}}S/v = F/v \qquad (1.59)$$

В силу отсутствия сдвига по фазе между звуковым давлением и колебательной скоростью сопротивление излучения является активным.

С введением понятий удельного акустического сопротивления и сопротивления излучения выражения для силы звука и излучаемой акустической мощности принимают вид:

$$\begin{aligned} I &= p_{\text{зв}}v = v^2 z_{\text{а}} = p^2_{\text{зв}.m}/2z_{\text{а}}; \\ P &= IS = v^2 z_{\text{а}}S = v^2 z_R. \end{aligned} \qquad (1.60)$$

1.4.1.5. Сферическая волна

Сферическая волна в идеальном случае создается пульсирующим шаром с радиусом R (рис. 1.28), звуковая энергия которого распространяется равномерно по всем направлениям, или иными словами – звуковые лучи по направлению совпадают с радиусами сферы.

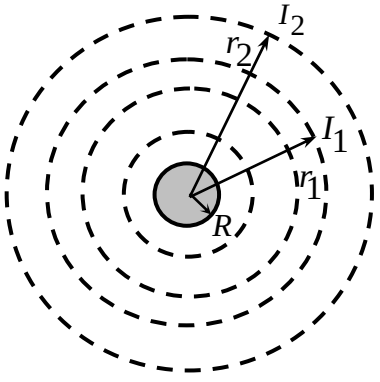


Рис. 1.28. Излучение сферической волны

Сила звука I_1 на поверхности фронта сферической волны (рис. 1.28) согласно [36] определяется как

$$I_1 = \frac{P}{S_1} = \frac{P}{4\pi r_1^2},$$

где P – излучаемая мощность, S_1 – площадь фронта волны, r_1 – расстояние от центра излучателя.

На расстоянии r_2 сила звука

$$I_2 = \frac{P}{S_2} = \frac{P}{4\pi r_2^2}.$$

Из двух последних выражений следует, что сила звука в сферической волне убывает обратно пропорционально квадрату расстояния от излучателя.

В пространстве положение точки можно определять в декартовой системе координат *X, Y, Z,* или в полярной системе координат (рис. 1.29). В последнем случае получаются более простые выражения, так как положение произвольной точки *O* в пространстве определяется радиусом-вектором *r*, азимутом Ψ и углом Θ между радиусом-вектором и осью *Z*. Так как фронт волны представляет собой сферическую поверхность, то все точки среды, находящиеся на такой поверхности будут колебаться синфазно с одинаковой амплитудой. Значения амплитуды и фазы колебаний будут зависеть только от расстояния от источника звука.

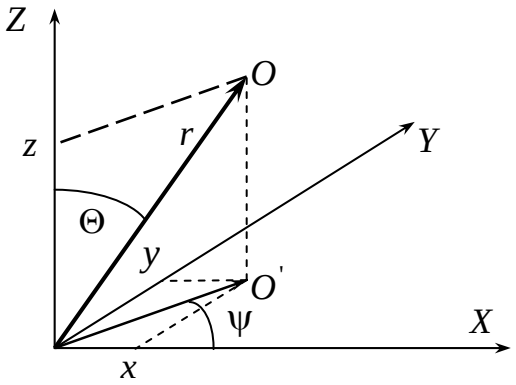


Рис. 1.29. Определение положения точки пространства в различных системах координат

Для произвольного значения *r* можно записать выражения для звукового давления

$$p_{\text{зв}} = p_{\text{зв}.m} e^{j(\omega t - kr)} \qquad (1.61)$$

и для интенсивности звука

$$I = \frac{P}{S} = \frac{P}{4\pi r^2}. \qquad (1.62)$$

С другой стороны согласно (1.60) $I = p_{\text{зв}.m}^2 / 2z_{\text{а}}$. Приравнивая выражения (1.60) и (1.62) для силы звука, получим

$$\frac{P}{4\pi r^2} = \frac{p_{\text{зв}.m}^2}{2z_{\text{а}}},$$

откуда определим амплитуду звукового давления как

$$p_{\text{зв}.m} = \sqrt{\frac{2Pz_{\text{а}}}{4\pi r^2}} = \frac{1}{r}\sqrt{\frac{Pz_{\text{а}}}{2\pi}} = \frac{A}{r}, \qquad (1.63)$$

где $A = \sqrt{\frac{Pz_a}{2\pi}}$.

Подстановкой (1.63) в (1.61) определим давление в произвольной точке пространства:

$$p_{\text{зв}} = \frac{A}{r} e^{j(\omega t - kr)}. \qquad (1.64)$$

Для определения колебательной скорости рассмотрим совместно выражения для уравнения движения (1.51) и звукового давления (1.64). Из уравнения движения следует, что $dv = -\frac{1}{\rho} \cdot \frac{dp_{\text{зв}}}{dr} dt$, а

$$\frac{d\,p_{зв}}{dr}=\frac{d}{dr}\left[\frac{A}{r}e^{j(\omega t-kr)}\right]=\frac{A}{r}(-jk)e^{j(\omega t-kr)}-\frac{A}{r^2}e^{j(\omega t-kr)}. \qquad (1.65)$$

После интегрирования уравнения движения с учетом (1.65) и упрощения приведем окончательный результат согласно [37]:

$$v=\frac{p_{зв}}{z_a\cos\varphi}e^{-j\varphi}, \qquad (1.66)$$

где фазовый сдвиг $\varphi=\operatorname{arctg}\frac{1}{kr}$.

Анализ выражений (1.64) и (1.66) показывает, что:

1. Амплитуды звукового давления и колебательной скорости обратно пропорциональны расстоянию от излучателя. Это связано с тем, что площадь фронта звуковой волны увеличивается по мере удаления от излучателя, а, следовательно, уменьшается звуковая энергия на единицу площади.

2. Колебательная скорость отстает по фазе от давления. В ближней зоне (при выполнении условия $r<<\lambda$) фазовый сдвиг значителен и у поверхности излучателя $\varphi=90°$. В дальней зоне фазовым сдвигом можно пренебречь.

1.4.1.6. Акустические и электрические уровни

В акустике в силу большого диапазона изменения акустических параметров звука и логарифмического закона восприятия слышимых звуков результаты измерений принято представлять в относительных логарифмических единицах. Для измерения слуховых ощущений была предложена единица *децибел* (дБ), равная 0,1 *бела* (Б). Параметры, измеренные в децибелах, называются *уровнями*. Различают относительные, абсолютные, акустические и электрические уровни.

За уровень L энергетических параметров k (интенсивности звука, электрической мощности и др.) принимают $L=10\lg(k/k_0)$, где k – измеряемый параметр, k_0– некоторое значение параметра, принимаемое за нулевой уровень. Так при оценке уровня интенсивности L_I за нулевой уровень принимают интенсивность I_0, близкую к пороговой интенсивности для нормального слуха на частоте 1000 Гц и равной 10^{-12} Вт/м^2, а уровень интенсивности

$$L_I=10\lg(I/I_0). \qquad (1.67)$$

Уровень плотности энергии, которая прямо пропорциональна интенсивности, определяется по формуле

$$L_\varepsilon=10\lg(\varepsilon/\varepsilon_0), \qquad (1.68)$$

где $\varepsilon_0 = I_0/c = 10^{-12}/333 \approx 3\cdot10^{-15}$ Дж/м^3 – нулевой уровень плотности энергии.

Под уровнем линейного параметра (звукового давления, напряжения, тока и др.) понимают величину

$$L = 20\lg(k/k_0). \quad (1.69)$$

Уровень звукового давления

$$L_p = 20\lg(p_{зв}/p_{зв0}), \quad (1.70)$$

где $p_{зв0} = 2\cdot10^{-5}$ *Па*.

Электрические уровни разделяют на уровни мощности

$$L_p = 10\lg(P/P_0), \quad (1.71)$$

уровни напряжения

$$L_U = 20\lg(U/U_0), \quad (1.72)$$

уровни тока

$$L_I = 20\lg(I/I_0), \quad (1.73)$$

где $P_0 = 1$мВт, а при рассеянии этой мощности на сопротивлении 600 *Ом* получим $U_0 = 0{,}775$ В, $I_0 = 1{,}29$ мА.

При вычислении абсолютных электрических уровней прибегают к добавлению к сокращенному обозначению децибела начальной буквы соответствующей величины, например, дБн указывает на абсолютный уровень напряжения, а дБм – на абсолютный уровень мощности. Кроме того, размерности дБ/В, дБ/мВ, дБ/мкВ, дБ/Вт обозначают относительные уровни напряжения и мощности, вычисленные относительно 1 В, 1 мВ, 1мкВ, 1 Вт.

1.4.1.7. Звуковые сигналы

Все звуки разделяются на несколько групп [36].

Чистые тоны. Чистые тоны имеют место, если звуковое давление является гармонической функцией с постоянными частотой, амплитудой и начальной фазой. На слух тоны воспринимаются в зависимости от частоты и амплитуды как тихие или громкие, высокие или низкие.

Созвучие. Созвучие представляет собой стационарный звук, состоящий из нескольких тонов. В большинстве случаев под созвучием понимают комбинацию основного тона и нескольких обертонов с кратными частотами. Звуковое давление созвучия описывается периодической несинусоидальной функцией времени, что можно рассматривать как сумму определенных гармоник ряда Фурье.

Амплитудно-модулированные тоны. Амплитудно-модулированные (АМ) тоны являются нестационарными сигналами постоянной (несущей) частоты, амплитуда которых является функцией времени. Спектр АМ колебаний имеет несущую частоту и две боковые составляющие. Модулирующий сигнал может иметь как гармоническую, так и любую другую форму.

Частотно-модулированные тоны. Характеристиками частотно-модулированного (ЧМ) сигнала являются несущая частота, модулирующая частота, девиация несущей частоты (пределы изменения) и индекс модуляции – отношение девиации к модулирующей частоте. Чем больше индекс модуляции, тем больше боковых составляющих в частотном в спектре. При небольших индексах спектр ЧМ-сигналов такой же, как и у АМ-сигналов.

Частотный интервал между составляющими спектра ЧМ сигналов равен модулирующей частоте.

Биения. Если два тона имеют одинаковые частоты и амплитуды, то при изменении разности фаз сигналов возникает биение, которое на слух воспринимается как периодическое изменение громкости тона.

Шумы. Звуки с непрерывным спектром называются шумами. По типу огибающей амплитудно-частотного спектра шумы подразделяются на белый, розовый и равномерно маскирующий. В зависимости от ширины частотного спектра шумы могут быть широкополосными, узкополосными, октавными, третьоктавными и др.

Белый шум характеризуется спектральной плотностью мощности, не зависящей от частоты. При линейной шкале частоты белому шуму соответствует характеристика 1 (рис. 1.30, а). Она располагается горизонтально во всем частотном диапазоне. В октавной шкале частот эта характеристика принимает вид прямой с подъемом +3 дБ на октаву в сторону более высоких частот.

Розовый шум. У сигналов розового шума спектральная плотность мощности в линейной шкале частот имеет вид наклонной прямой, спадающей к области высоких частот (прямая 2 на рис. 1.30, *а*). В октавной шкале спектральная плотность мощности розового шума представляет собой горизонтальную линию.

Равномерномаскирующий шум. В области частот 0…500 Гц характеризуется свойствами белого шума, а после этого диапазона соответствует свойствам розового шума (характеристика *3* на рис. 1.30, *а*).

Одинаковая маскировка во всем звуковом диапазоне частот обусловлена тем, что критические полосы слуха до 500 Гц по ширине примерно одинаковы, а далее с ростом частоты их полоса линейно растет. При восприятии звука слуховой аппарат человека разделяет его на критические полосы (или частотные группы) слуха. В диапазоне частот от 20 до 16000 Гц число критических полос равно 24.

Ширина критических полос слуха не связана с уровнем интенсивности сигнала. На частотах до 500 Гц ширина частотных групп $\Delta F_{\text{кр}}$ равна примерно 100 Гц. На частотах более 500 Гц ширина частотных групп увеличивается пропорционально средней частоте $F_{\text{ср}}$, причем соблюдается постоянство отношения $\Delta F / F_{\text{ср}} = 0{,}2$.

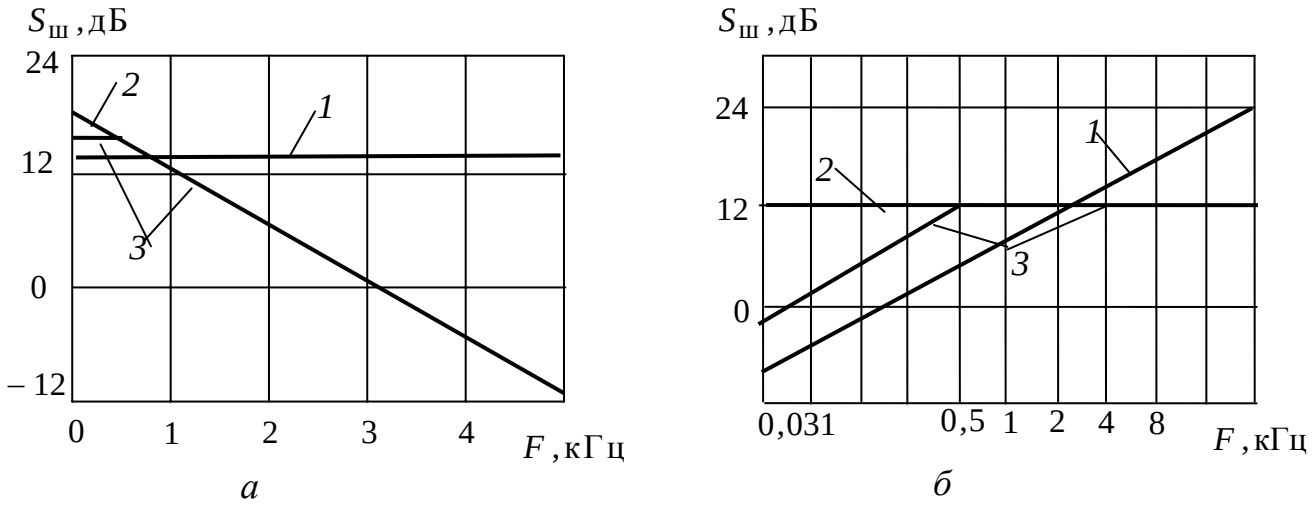


Рис. 1.30. Частотные характеристики спектральной плотности мощности шумов: *а* – в линейной шкале частот; *б* – в октавной шкале частот; *1* – белый шум, *2* – розовый шум, *3* – равномерно маскирующий шум

График зависимости ширины критической полосы слуха от ее средней частоты приведен на рис. 1.31.

На интервалах частотных групп слух интегрирует возбуждение по частоте и не реагирует на особенности структуры возбуждения. По этой же причине слух воспринимает не общую мощность шума, а только мощность шума в критических полосах слуха.

При воздействии широкополосного шума слуховой анализатор выделяет из сплошного спектра дискретный спектр, число составляющих которого равно числу критических полос слуха.

Равномерно маскирующий шум можно сформировать специальным фильтром из сигнала белого шума.

Частотные характеристики спектральной плотности мощности шумов в октавной шкале частот показаны на рис. 1.30, *б*.

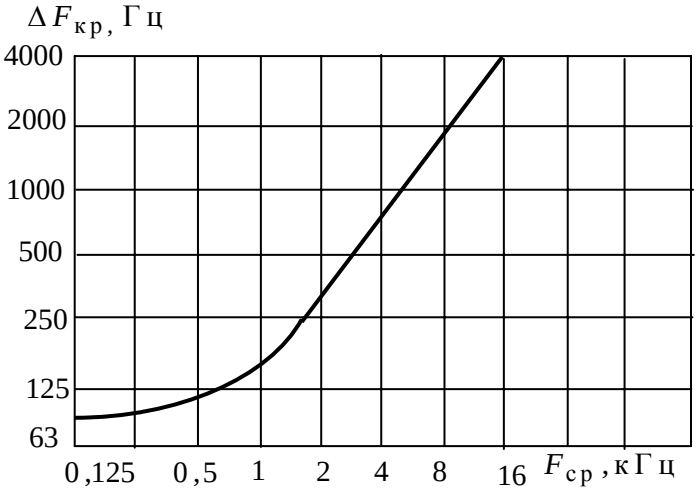


Рис. 1.31. Зависимость ширины критической полосы слуха от ее средней частоты

1.4.1.8. Маскировка звуковых сигналов

Маскировка звуковых сигналов является радикальным средством нейтрализации акустических каналов утечки речевой информации. Для эффек-

тивного применения технических средств защиты речевой информации необходимо подробное изучение особенностей методов маскировки информационных звуковых сигналов, проникающих за пределы контролируемой зоны из помещений, в которых циркулирует защищаемая речевая информация.

При одновременном воздействии на слух двух сигналов один из них может быть неразличим на фоне другого. В тишине хорошо слышимы слабые звуки, а в шуме могут быть неразличимы даже громкие звуки, т.е. при шуме порог слышимости для слабых звуков увеличивается. Повышение порога слышимости называют *маскировкой*. Величина маскировки определяется формулой [37]

$$M = L_{\text{псш}} - L_{\text{пст}}, \qquad (1.74)$$

где $L_{\text{псш}}$ и $L_{\text{пст}}$ – уровни порогов слышимости в шумах и в тишине.

Порогом слышимости называют наименьшее значение раздражающей силы (звукового давления) чистого тона, которое вызывает ощущение звука. Порог слышимости определяется значением частоты: при 1000 Гц он равен примерно 10^{-12} Вт/м^2. Этот порог характеризует чувствительность слуха к интенсивности звуковой энергии.

Абсолютный порог слышимости представляет собой порог, измеренный в полной тишине для гармонического сигнала. Он определен как среднестатистическая величина для людей в возрасте 18–20 лет при воздействии сигнала длительностью не менее 250 мс. Кривая уровня абсолютного порога слышимости показана на рис. 1.32 [36]. Нулевому уровню соответствует звуковое давление $2 \cdot 10^{-5}$ Па.

Пороги слышимости разные для левого и правого уха и зависят от возраста. На частоте 10 кГц чувствительность уха 60-летнего человека на 20 дБ ниже, чем у 20-летнего.

При давлении 60…80 Па человек ощущает давление на уши. Эта величина давления называется порогом осязания.

Давление более 150…200 Па вызывает болевые ощущения в органах слуха и называется болевым порогом (рис. 1.32)

Слуховая система человека адаптирована к звукам малой и средней силы с уровнем давления не выше 94…96 дБ. Звуки с уровнем давления более 75 дБ при длительном воздействии могут привести к полной глухоте.

В направлении низких частот со значения 500 Гц порог слышимости резко возрастает и для слухового ощущения требуется более высокое звуковое давление (рис. 1.33). На частоте 100 Гц порог слышимости по звуковому давлению в 10^4 раз больше, чем на частоте 1000 Гц. В направлении более высоких частот порог слышимости сначала снижается (в 8–10 раз на частотах 2–4 кГц), а затем начинает повышаться так же, как и в низкочастотном диапазоне.

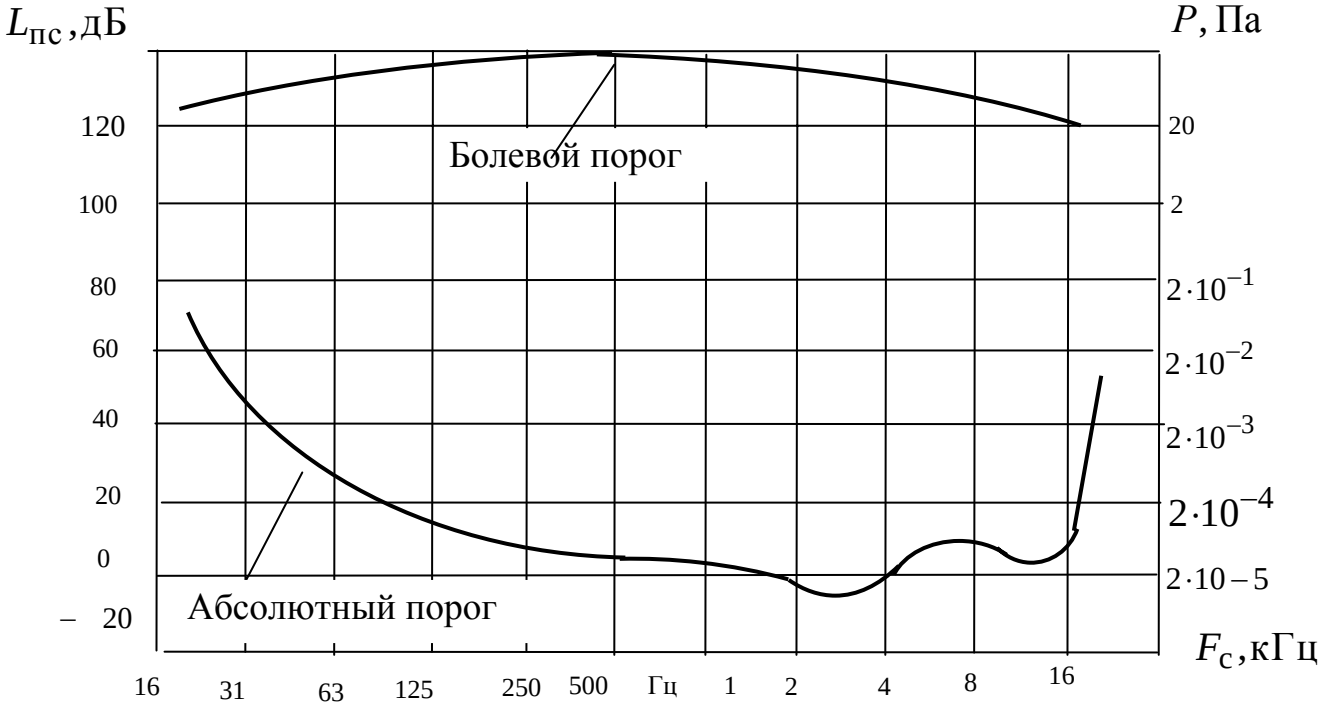


Рис. 1.32. Кривые абсолютного и болевого порогов слышимости

Уровень звукового давления характеризует объективно только физические процессы, но из выше рассмотренного следует, что звуки одинаковой интенсивности в различных частотных диапазонах могут быть слышимыми и неслышимыми. Для оценки восприятия звука служит характеристика, называемая уровнем слухового ощущения:

$$E = 10\lg\frac{I}{I_{пс}} = 10\lg\frac{I}{I_0} - 10\lg\frac{I_{пс}}{I_0} = L_I - L_{пс}, \qquad (1.75)$$

где $L_{пс}$ – уровень интенсивности звука на пороге слышимости.

Из полученного выражения следует, что уровень ощущения представляет собой ту часть уровня интенсивности звука, которая находится над уровнем порога слышимости на той же частоте. При изменении порога слышимости изменяется и уровень ощущения E.

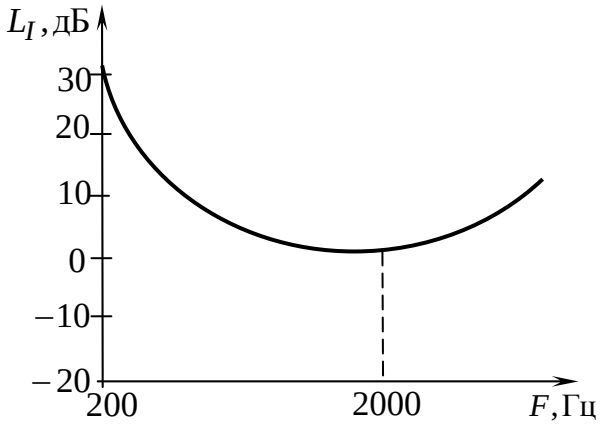


Рис. 1.33. Порог слышимости по давлению около ушной раковины

При интенсивности звука I в условиях приема в шумах уровень ощущения звука $E_ш$ с учетом (1.74) определяется как

$$E_ш = 10\lg\frac{I}{I_{псш}} = 10\lg\frac{I/I_0}{I_{псш}/I_0} = L_I - L_{псш} = L_I - L_{пст} - M = E_т - M, \qquad (1.76)$$

где $I_{\text{псш}}$ – интенсивность на пороге слышимости при наличии помех и шумов; $E_{\text{т}}$ – уровень ощущения того же звука в тишине.

Выражение (1.76) показывает, что с возрастанием уровня шума снижается уровень ощущения. Четкое ощущение воспринимаемого звука имеет место при превышении уровнем принимаемого звука уровня составляющих помехи в одной и той же полосе слуха.

Низкочастотные тоны сильнее маскируют высокочастотные в силу особенностей устройства слухового аппарата человека. Если шум широкополосный, то даже при большом превышении его общего уровня над уровнем воспринимаемого тона последний может быть услышан, поскольку уровень шума в критической полосе этого тона может быть достаточно малым.

Для низких уровней ширина полосы частот маскировки относительно мала, для высоких уровней ширина полосы лежит в широкой области частот, лежащих выше частоты маскирующего тона. При этом имеет место повышение маскировки на частотах, кратных частоте маскирующего тона. Экспериментально установлено [37], что при воздействии чистого тона с уровнем интенсивности 100 дБ человек слышит вторую гармонику с уровнем интенсивности 88 дБ, третью – с уровнем 74 дБ и т.д., хотя высшие гармоники в чистом тоне отсутствуют. Наличие высших гармоник в слуховом ощущении можно проверить экспериментально следующим образом: к уху дополнительно подводится источник звука другого чистого тона с плавно перестраиваемой частотой. На каждой кратной основному тону частоте человеком прослушиваются биения, как будто в подводимом звуке были высшие гармоники. Эти гармонические составляющие называются субъективными. Именно они обеспечивают маскировку звука на кратных маскирующему тону частотах.

Причина прослушивания высших гармоник чистого тона, по-видимому, заключается в нелинейных свойствах слухового тракта человека, искажающего входной звуковой сигнал.

При воздействии на органы слуха двух тонов различных частот, не попадающих в одну полосу слуха, человек может прослушивать тон разностной частоты с достаточной громкостью и тон суммарной частоты, а также и других комбинационных частот $F = mF_1 \pm nF_2$ с меньшими уровнями.

При воздействии на слух сложных звуков с составляющими на кратных частотах человек ощущает такой же звук по частотному составу, но с измененным соотношением амплитуд составляющих частотного спектра в результате совпадения комбинационных частот с исходными частотами.

Маскировка чистым тоном. Напомним, что маскировка согласно (1.74) определяется в децибелах как разность уровней порогов слышимости в шумах и в тишине (абсолютный порог слышимости).

Для случая маскировки чистым тоном уровень порога слышимости $L_{пс}$ звукового сигнала с частотой $F_с$ определяется по соответствующим графикам (рис. 1.34) при действии мешающего чистого тона с частотой $F_м$ для разных уровней $L_м$ интенсивности маскирующего тона.

Особенности маскировки чистым тоном заключаются в следующем [36]:

- максимальный эффект маскировки имеет место, если частоты $F_с$ и $F_м$ близки по значению; чем больше разнос частот, тем меньше маскирующее действие;
- эффект маскировки тем выше, чем выше уровень интенсивности маскирующего тона;
- кривые маскировки имеют более пологий спад в сторону высоких частот, поэтому более высокие частоты лучше маскируются чистым тоном, чем более низкие.

На частотах $F_с$, кратных частоте маскирующего тона $F_м$, возникают биения (провалы в графиках), причина появления которых была объяснена ранее.

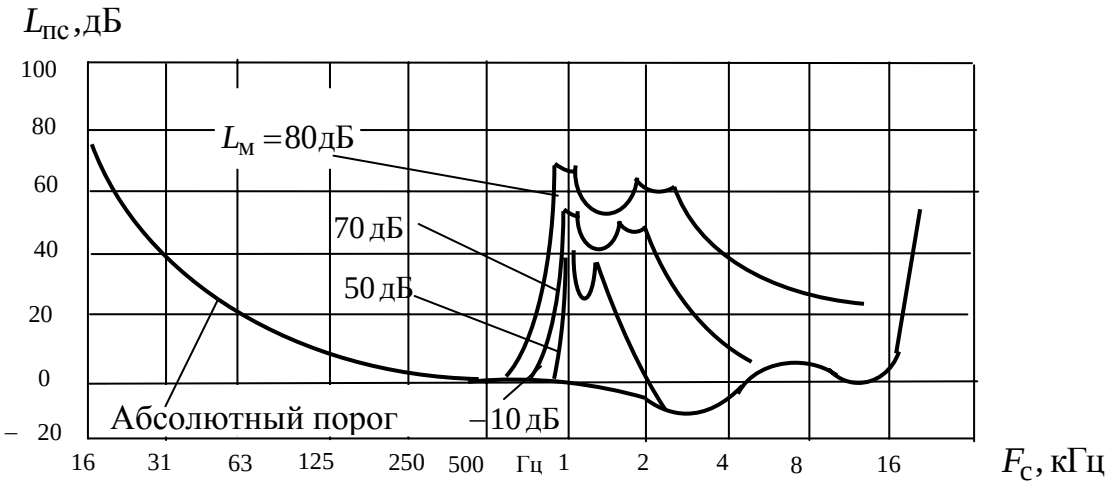


Рис. 1.34. Кривые порога слышимости тона с частотой $F_с$ при маскировке тоном $F_м$ с частотой 1000 Гц для разных уровней интенсивности маскирующего тона

Маскировка узкополосным шумом. В целом кривые порога слышимости имеют такой же характер, как и в предыдущем случае, только отсутствуют биения справа и несколько шире диапазон маскируемых частот.

Сигналы, спектр которых лежит на октаву ниже центральной частоты 1 кГц маскирующего шума, практически не маскируются.

Маскировка широкополосным белым шумом. Маскировка белым шумом наиболее распространена при защите речевой информации.

Кривые порога слышимости тона с частотой $F_с$ при маскировке белым шумом показаны на рис. 1.35.

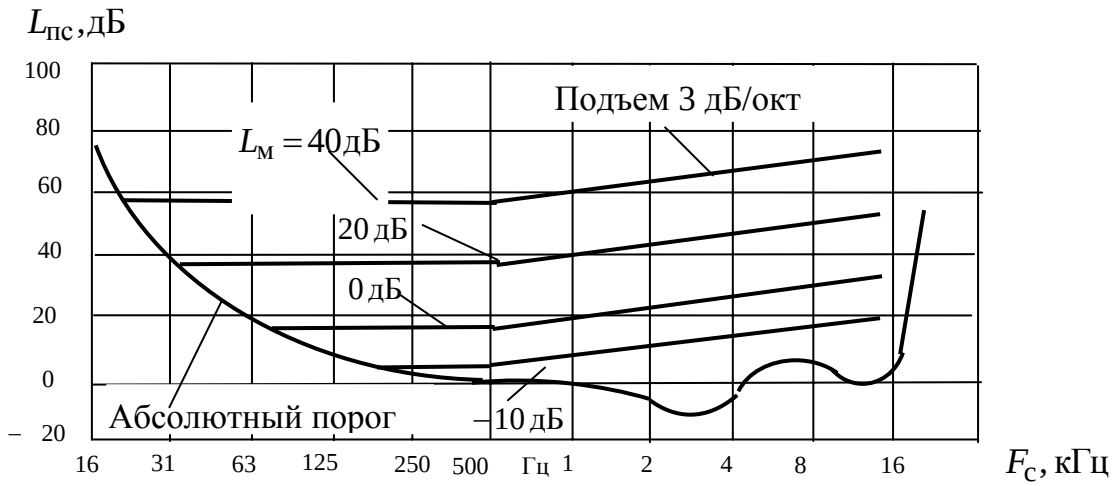


Рис. 1.35. Кривые порога слышимости тона с частотой $F_с$ при маскировке белым шумом

Характерные особенности кривых заключаются в следующем:

- до частоты 500 Гц кривые располагаются горизонтально;
- с увеличением частоты свыше 500 Гц порог маскировки линейно повышается на 3 дБ/октаву.

Так как слух реагирует не на общую энергию сигнала, а на энергию в критических полосах слуха, которые до 500 Гц по ширине примерно одинаковы, то маскировка в этом звуковом диапазоне одинакова, т. е. порог слышимости от частоты не зависит. Далее с ростом частоты их критические полосы линейно растут, их ширина пропорциональна средней частоте. В этом диапазоне при увеличении частоты в 10 раз порог слышимости возрастает на 10 дБ.

Маскировка равномерно маскирующим шумом. Шум, обеспечивающий одинаковую маскировку во всем частотном звуковом диапазоне, называется равномерно маскирующим. Кривые маскировки показаны на рис. 1.36.

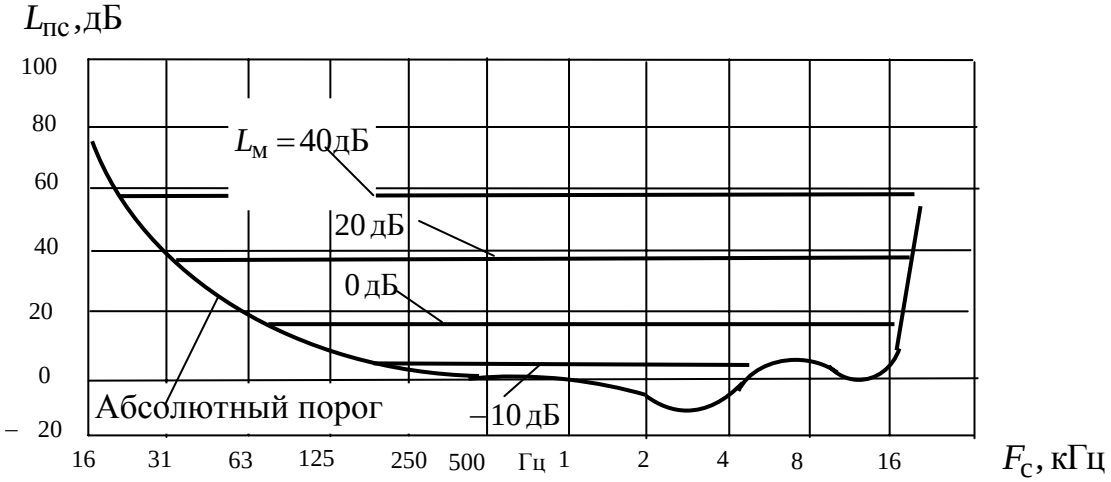


Рис. 1.36. Кривые порога слышимости тона с частотой $F_с$ при равномерно маскирующем шуме

До частоты 500 Гц равномерно маскирующий шум должен иметь спектральную плотность мощности такую же, как у белого шума. В области более высоких частот спектральная плотность мощности должна уменьшаться пропорционально частоте как у розового шума.

1.4.2. Понятность и разборчивость речи

Основной характеристикой любого канала передачи речи является понятность речи. Для определения этой характеристики применяется статистический метод с участием большого числа слушателей и дикторов. Разработан косвенный количественный метод определения понятности речи через ее разборчивость. Под разборчивостью речи понимают относительное или процентное количество принятых (понятых) элементов речи из общего числа переданных по каналу. Элементы речи составляют слоги, звуки, слова, фразы, цифры. В соответствие им поставлены слоговая, звуковая, словесная, смысловая и цифровая разборчивость. Преимущественное применение на практике получили слоговая, звуковая и словесная разборчивость. Для измерения разборчивости разработаны артикуляционные таблицы слогов, звукосочетаний и слов с учетом встречаемости их в русской речи.

Измерение разборчивости производится с помощью артикуляционной группы тренированных слушателей и дикторов без нарушения слуха и речи, поэтому и метод называется артикуляционным.

Для определения связи между разборчивостью, измеренной артикулянтами, и понятностью речи для обычных людей были проведены массовые испытания. Разговор велся по специальным разговорникам в обе стороны, как при телефонных переговорах. При этом контролировалось понимание абонентами друг друга. Оценка понятности ставилась по пятибальной системе. Одновременно для каждого из условий испытаний и каждого тракта были измерены величины разборчивости речи с помощью тренированной бригады.

В таблице приведены градации понятности речи и соответствующие им разборчивости [37].

Понятность	Разборчивость, %	
	Слоговая	Словесная
Предельно допустимая	25–40	75–87
Удовлетворительная	40–50	87–93
Хорошая	50–80	93–98
Отличная	80 и выше	98 и выше

Одновременно с указанными испытаниями были измерены статистические зависимости между слоговой, словесной, звуковой и смысловой разборчивостью для русского языка.

Формантная теория, разработанная Флетчером и Коллардом, позволила установить непосредственную связь между разборчивостью речи и характеристиками тракта передачи речи [37, 42].

Звуковые единицы характеризуются различными свойствами в зависимости от различных факторов их рассмотрения. Образованию звуковых единиц соответствует артикуляционный фактор, который называют анатомо-физиологическим. Акустический фактор относится к свойствам звуковых единиц в результате работы произносительных органов и определяет звучание речи. Восприятие звуков человеком относится к перцептивному фактору.

Первоначально описания звуковых систем осуществлялось на основе анализа артикуляций. Но с развитием техники акустического анализа звуков исследователи приходят к выводу, что акустические характеристики речи наиболее важны. Современная фонетика учитывает тесную связь и взаимообусловленность между артикуляционными и акустическими характеристиками речи.

Исследования восприятия речевых единиц показывает, что они воспринимаются не так, как любые другие звуки. Это объясняется как способностью человека преобразовывать их в соответствующие артикуляции, так и функциональными свойствами речевых звуковых единиц.

Звуки речи являются сложными звуками в основном из-за того, что процесс речеобразования сопровождается резонансными явлениями, собственные частоты которых изменяются в зависимости от того, какой звук в данный момент произносится.

Источник звука вызывает в системе резонаторов речеобразующего тракта собственные колебания. Звуки на собственных частотах резонаторов являются наиболее усиленными. Собственные частоты резонаторов называют формантами звука, так как они формируют характерное звучание гласных и согласных.

Частоты формант определяются конфигурацией речевого тракта и свойства источника звука на них не влияет. Это одно из важнейших положений акустической теории речеобразования. Это положение позволяет связывать частоты формант только со спецификой артикуляции и по частотам формант судить о положении артикуляционных органов.

Число формант, существенно характеризующих определенный звук речи, исследователи определяют по разному, но в большинстве случаев исследователи считают, что в образовании определенного звука участвуют четыре форманты.

Форманты звуков речи заполняют весь частотный диапазон от 150 до 7000 Гц. Средняя вероятность появления формант в том или ином участке частотного диапазона для каждого языка вполне определенна. Условились делить весь частотный диапазон на 20 полос (в том числе и для русского

языка) с одинаковой вероятностью появления формант в каждой из них. Соответствующие полосы назвали полосами равной разборчивости. Оказалось, что при достаточно большом объеме передаваемой речи вероятности появления формант подчиняются правилу аддитивности. Вследствие этого вероятность появления формант в каждой полосе равной разборчивости равна 0,05.

Если воспринимать речь в условиях шумов и помех, то ее разборчивость получается меньшей. Это связано с тем, что форманты имеют различные уровни интенсивности: у громких звуков выше, чем у глухих. Поэтому при повышении уровня шумов сначала маскируются форманты с низкими уровнями, а затем с более высокими. При увеличении уровня шумов и помех вероятность восприятия формант постепенно уменьшается. Коэффициент, определяющий это уменьшение, называют коэффициентом восприятия или коэффициентом разборчивости w. В каждой полосе равной разборчивости вероятность приема формант будет $\Delta A = 0{,}05w$.

Так как вся энергия звуков речи в основном сосредоточена в формантах, то уровни формант практически совпадают с уровнями звуков речи.

Порог слышимости в шумах определяется спектральными уровнями шумов. Разность между средним спектральным уровнем речи и спектральным уровнем шумов будет определять вероятность появления формант выше уровня шумов.

Коэффициент разборчивости w определяется уровнем ощущения формант

$$E = B_{\text{р}} - B_{\text{ш}}, \tag{1.77}$$

где $B_{\text{р}}$ – средний спектральный уровень речи; $B_{\text{ш}}$ – спектральный уровень шумов.

Для уровней ощущения, находящихся в пределах 0–18 дБ, коэффициент разборчивости можно определить по приближенной формуле $w = (E + 6)/30$.

Для каждой полосы равной разборчивости коэффициент разборчивости (w_n) будет разным. Тогда суммарная вероятность приема формант (разборчивость формант) определяется как

$$A_{\text{ф}} = \sum_{n=1}^{20} 0{,}05 w_n. \tag{1.78}$$

1.4.3. Частотный диапазон и спектры

Акустические сигналы от источников звука в большинстве случаев имеют непрерывно изменяющиеся форму и частотный спектр. Спектры могут быть низкочастотными, высокочастотными, дискретными и непре-

рывными. Даже у однотипных источников звука спектры имеют индивидуальные особенности, определяющие окраску звука, называемую тембром.

Понятие высоты звука отражает субъективную оценку восприятия звука по частотному диапазону. Как отмечалось ранее, ширина критических полос слуха на средних и высоких частотах примерно пропорциональна частоте, поэтому субъективный масштаб восприятия звука по частоте примерно соответствует логарифмическому закону. По этой причине все частотные характеристики устройств передачи звуков представляют в логарифмическом масштабе.

За объективную единицу высоты звука принята октава – отрезок равномерной шкалы, начальное и конечное значения частоты на котором отличаются в два раза. Октаву делят на части: полуоктавы и третьоктавы (рис. 1.37).

Для третьоктав стандартизован ряд частот в килогерцах (рис. 1.37): 1; 1,25; 1,6; 2; 2,5; 3,15; 4; 5; 6,3; 8; 10.

Основной интерес представляют средний спектр для источников звука. Он может быть сплошным и иметь достаточно сглаженную форму.

Сплошные спектры характеризуют зависимость спектральной плотности от частоты. Эту зависимость называют также энергетическим спектром. Спектральной плотностью называется интенсивность звука в полосе частот шириной, равной единице частоты. Для акустики эту полосу берут равной 1 Гц. Спектральная плотность $J = I_{\Delta f} / \Delta f$, где $I_{\Delta f}$ – интенсивность звука, измеренная в узкой полосе Δf с помощью узкополосных фильтров.

В акустике введена логарифмическая мера плотности – спектральный уровень

$$B = 10\lg(J / I_0), \qquad (1.79)$$

где $I_0 = 10^{-12}$ Вт/м^2 – интенсивность звука, соответствующая нулевому уровню.

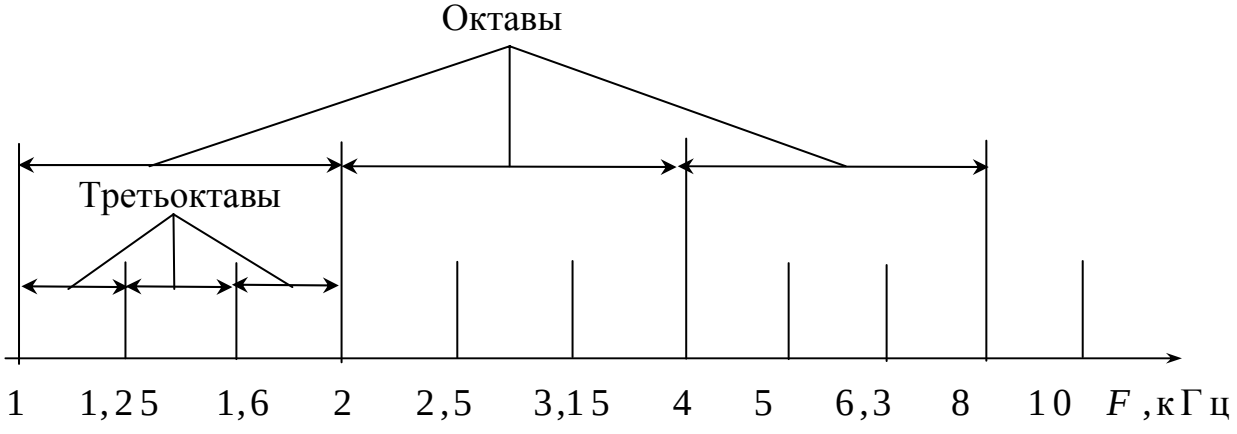


Рис. 1.37. Октавная и третьоктавная шкалы частот

В качестве характеристики спектра можно вместо спектральной плотности использовать интенсивности и уровни интенсивности, измеренные в октавной, полуоктавной и третьоктавной полосе частот. Связь между спектральным уровнем и уровнем в октавной (полуоктавной или третьоктавной) полосе можно установить, записав (1.79) в виде

$$B = 10\lg(J/I_0) = 10\lg(I_{\Delta f\ \text{окт}}/\Delta f_{\text{окт}} I_0) \qquad (1.80)$$

и определив уровень в октавной полосе как

$$L_{\text{окт}} = 10\lg(I_{\Delta f\ \text{окт}}/I_0). \qquad (1.81)$$

Вычитая выражение (1.80) из (1.81), определяем

$$L_{\text{окт}} - B = 10\lg(I_{\Delta f\ \text{окт}}/I_0) - 10\lg(I_{\Delta f\ \text{окт}}/\Delta f_{\text{окт}} I_0) = 10\lg\frac{I_{\Delta f\ \text{окт}}\Delta f_{\text{окт}} I_0}{I_0 I_{\Delta f\ \text{окт}}} = 10\lg\Delta f_{\text{окт}} \qquad (1.82)$$

При известном спектре сигнала можно определить его суммарную интенсивность. Если спектр задан в уровнях интенсивности для третьоктавных полос, то необходимо пересчитать эти уровни в каждой из полос в интенсивности $I_{\text{окт}} = I_0 10^{0,1L_{\text{окт}}}$, а затем просуммировать все интенсивности [37]. Сумма всех составляющих $I_{\text{окт}}$ дает суммарную интенсивность $I_{\text{сум}}$ для всего спектра. Суммарный уровень определяется как

$$L_{\text{сум}} = 10\lg(I_{\text{сум}}/I_0). \qquad (1.83)$$

Приближенно суммарный уровень можно определить делением частотного диапазона на n полосок шириной Δf_k, в пределах которых спектральный уровень B_k примерно постоянен, и вычислением по формуле

$$L_{\text{сум}} \approx 10\lg\sum_{k=1}^{n} 10^{0,1B_k}\Delta f_k. \qquad (1.84)$$

1.4.4. Звуковое поле в помещении

В закрытых помещениях звуковые волны многократно отражаются от ограждающих поверхностей, в результате чего создается сложная картина звукового поля. Законы распределения характеристик звукового поля в данной ситуации определяются не только свойствами источника звука, но и другими факторами – геометрией помещения; способностью стен, потолка и пола поглощать и отражать звуковую энергию. Поэтому звуковые поля в закрытом помещении и в свободном пространстве имеют различные структуры. Если в свободном пространстве интенсивность звука определяется потоком энергии в направлении распространения волны, то в помещении результирующий поток энергии имеет две составляющие – прямой поток и отраженный (иногда многократно) поток. Направление потоков

энергии отраженных волн зависит от особенностей планировки помещения и степени поглощения звуковой энергии поверхностями ограждающих конструкций. В этой ситуации определение интенсивности звука в классическом понимании неприменимо.

Приемлемой энергетической характеристикой звукового поля в помещении является плотность звуковой энергии ε.

Если помещение не содержит фокусирующих поверхностей и геометрически симметричных сечений, а размеры помещения значительно больше длины волны и если ограждающие конструкции не сильно поглощают звуковую энергию, то через некоторое время при непрерывном действии источника звука через произвольный элемент сечения помещения в каждый момент времени будет проходить большое число отдельных волн, распространяющихся в разных направлениях. В результате звуковое поле будет характеризоваться следующими свойствами [36]:

- потоки энергии этих волн по всем направлениям равновероятны;
- плотность звуковой энергии ε звукового поля по всему объему помещения постоянна.

Равновероятность потоков энергии волн называют изотропией звукового поля, а постоянство звуковой энергии по объему помещения – однородностью. Если звуковое поле является изотропным и однородным, то его называют диффузным. Для диффузного поля характерно отсутствие явлений интерференции.

Процесс нарастания плотности звуковой энергии в помещении протекает очень быстро и незаметно для слуха. Процесс спада (поглощения) звуковой энергии, называемый реверберацией, протекает значительно медленнее и заметно для слуха. Реверберация влияет на слуховое восприятие.

Поглощение звуковой энергии осуществляется не только ограждающими конструкциями помещения, но и воздушной средой. Потери энергии в воздушной среде обусловлены вязкостью и теплопроводностью воздуха, а также молекулярным поглощением. Поглощение звуковой энергии воздухом зависит от пробега звуковой волны и определяется как

$$\varepsilon = \varepsilon_0 e^{-\mu l}, \qquad (1.85)$$

где $l = c_{зв} t$ – длина пробега звуковой волны; ε_0 – установившаяся плотность звуковой энергии в помещении; μ – коэффициент затухания, равный обратному значению пути, на котором плотность энергии уменьшается в e раз. Коэффициент затухания $\mu = 52{,}5\dfrac{F^2}{c\rho_0}\eta$ зависит от плотности ρ_0, вязкости η воздуха, частоты F, а также от температуры и влажности воздуха.

1.4.5. Звуковой фон в помещении

Звуковой фон в помещении образуют шумы, которые проникают в помещение от различных посторонних и внутренних источников. Из смежных помещений проникают шумы из-за звукопроводности строительных конструкций, ограждающих помещение. Шумы вибрационного происхождения образуются от работающих в здании машин и механизмов. Системы кондиционирования и вентиляции создают внутренние шумы, к которым можно отнести также шумы технологического оборудования (например, шумы вентиляторов компьютеров и других электронных устройств).

1.4.6. Характеристики помещения

Акустическое отношение. Общее звуковое поле в помещении определяется суммой полей «прямого» звука и звука отраженного от ограждающих конструкций. Поле отраженных волн в большинстве случаев можно считать диффузным. Отношение плотности энергии отраженных звуков к плотности энергии прямого звука $R = \varepsilon_{\text{диф}} / \varepsilon_{\text{пр}}$ называют акустическим отношением [37]. Акустическое отношение может быть выражено через звуковые давления как

$$R = p^2_{\text{диф}} \Big/ p^2_{\text{пр}}. \qquad (1.86)$$

Акустическое отношение, выраженное в уровнях, принимает вид

$$\Delta L_R = 10 \lg R = L_{\text{диф}} - L_{\text{пр}}. \qquad (1.87)$$

Отраженные звуковые волны можно отнести к помехам, поэтому акустическое отношение является важной характеристикой акустических свойств помещения в стационарных режимах. Акустическое отношение редко бывает меньше единицы, т.е. уровень отраженных волн в большинстве случаев выше уровня поля прямого звука.

Если в помещении источник звука с акустической мощностью $P_{\text{а}}$ создает диффузное звуковое поле, то плотность звуковой энергии будет определяться выражением $\varepsilon_0 = 4P_{\text{а}} / c_{\text{зв}} \alpha S$, откуда следует

$$P_{\text{а}} = \varepsilon_0 c_{\text{зв}} S \alpha / 4, \qquad (1.88)$$

где $\alpha = I / I_{\text{пад}}$ – среднее значение коэффициента звукопоглощения; I – интенсивность поглощаемой энергии; $I_{\text{пад}}$ – интенсивность падающей энергии; S – общая площадь.

Для определения части звуковой мощности $P''_{\text{а}}$, которая проникает из помещения через стену, можно воспользоваться выражением (35), заменив в нем коэффициент звукопоглощения α коэффициентом звукопроводности $\gamma_{\text{п}}$, а S – площадью преграды $S_{\text{п}}$:

$$P''_{\text{а}} = \frac{\varepsilon_0 c_{\text{зв}} S_{\text{п}}}{4} \gamma_{\text{п}} = \frac{I_{\text{зв}} S_{\text{п}}}{4} \gamma_{\text{п}}, \qquad (1.89)$$

где $I_{\text{зв}} = \varepsilon_0 c_{\text{зв}}$ – интенсивность звука, падающего на стену.

1.4.7. Звукопоглощающие материалы и конструкции

Отражение звуковых волн происходит из-за несогласованности волновых акустических сопротивлений граничащих сред. Согласно общей теории коэффициент отражения по звуковому давлению [37]

$$\beta_{\text{отр}} = \frac{p_{\text{отр}}}{p_{\text{пад}}} = \frac{\delta_{\text{отр}} - \delta_{\text{воз}}}{\delta_{\text{отр}} + \delta_{\text{воз}}} \qquad (1.90)$$

определяется волновым акустическим сопротивлением воздуха $\delta_{\text{воз}}$ и волновым акустическим сопротивлением отражающей среды $\delta_{\text{отр}}$. Из (37) следует, что отражающая способность среды тем больше, чем больше ее волновое сопротивление.

Отношение интенсивности отраженных звуковых волн $I_{\text{отр}}$ к интенсивности падающих волн $I_{\text{пад}}$ называется коэффициентом отражения по интенсивности $\alpha_{\text{отр}}$, а отношение поглощенной энергии к падающей, выраженное через интенсивности, называется коэффициентом поглощения $\alpha = I / I_{\text{пад}}$. Без учета дифракции справедливо равенство $\alpha = 1 - \alpha_{\text{отр}}$.

Звукопоглощающие материалы бывают сплошными и пористыми. По назначению они подразделяются на стеновые, облицовочные, для драпировки и специальные (мембранные и резонаторные конструкции).

Сплошные материалы. Это в основном твердые материалы (бетон, кирпич, мрамор и т.п.), имеющие акустическое сопротивление существенно больше сопротивления воздуха. Их коэффициенты поглощения очень малы, не более 0,05. Из мягких сплошных материалов в качестве облицовки применяется плотная резина, коэффициент поглощения которой находится в пределах 0,1.

Пористые материалы. К ним относятся штукатурки, облицовочные плиты с перфорацией и без нее, портьеры, ковры и т.п. Они применяются только для облицовки и драпировки. За ними вплотную или на некотором расстоянии располагаются ограждающие конструкции, имеющие сплошную структуру (перекрытия, стены). При воздействии на пористые материалы звуковых волн следует учитывать отражение звука как от лицевой поверхности, так и от тыльной с учетом поглощения звука в материале. Для хорошо проницаемых для звука материалов надо учитывать отражение звуковых волн от ограждающих конструкций, находящихся за пористым материалом. Если за ним находится твердая стена, то отраженные от стены

волны будут повторно проходить через материал в обратном направлении частично поглощаясь снова от потерь на трение в порах материала. Поглощение звуковой волны будет максимальным при размещении пористой перегородки на небольшом расстоянии от стены (на расстоянии четверти длины звуковой волны).

Если пористый материал облицовки имеет достаточно большую толщину, то коэффициент поглощения увеличивается по ряду причин. Так как акустическое сопротивление пористых материалов соизмеримо с сопротивлением воздуха, то отражение от них почти отсутствует. Звуковые волны испытывают в поглощающем материале большие потери из-за вязкости материала и трения частиц воздуха в порах, в результате чего волны достигают поверхности стены значительно ослабленными. При обратном движении звуковой волны в пористом материале будет также происходить поглощение энергии, что определяет увеличение коэффициента поглощения. На определенных частотах коэффициент поглощения может быть очень большим (см. табл. 1).

Существует много звукопоглощающих материалов с акустическим сопротивлением, близким к сопротивлению воздуха. На определенных частотах они имеют коэффициент поглощения, приближающийся к единице.

Эффективны с точки зрения звукопоглощения слоистые конструкции из пористых материалов, слои которых подбирают с учетом получения максимального коэффициента поглощения.

Таблица 1

Материалы	Коэффициент поглощения на частотах, Гц					
	125	250	500	1000	2000	4000
Стена, штукатуренная гипсом	0,013	0,015	0,020	0,028	0,040	0,050
Акустическая штукатурка типа АГШ-Б	0,99	0,78	0,73	0,76	0, 60	0,59
Ковер с ворсом 1 см на бетоне	0,09	0,08	0,21	0,27	0,27	0,37
Резиновый ковер толщиной 0,5 см	0,04	0,04	0,08	0,12	0,03	0,10
Линолеум	0,02	0,025	0,03	0,035	0,04	0,01
Сосновая панель	0,098	0,110	0,100	0,087	0,082	0,110
Стекло ординарной толщины	0,035	0,030	0,027	0,024	0,020	0,020
Щиты Бекеши (холст, натянутый по вате)	0,80	0,81	0,73	0,58	0,46	0,43

Резонансные (мембранные и перфорированные) конструкции. Резонансными звукопоглотителями могут служить тонкие перегородки из сплошных материалов, поглощение которых определяется интенсивностью

их колебаний как единого целого под воздействием звука. Звукопоглощение обусловлено потерей энергии на трение и максимально при резонансе. Мембранные конструкции представляют собой деревянные рамы с прикрепленными тонкими листами фанеры, пластмассы, полимерной пленки и т.п. Воздушный зазор между слоем и стеной иногда заполняют рыхлым пористым материалом. Перфорированные звукопоглотители представляют собой пористо-колебательные системы. Они содержат слой мягкого пористого материала, прикрепленного к стене и покрытого перфорированной пластиной.

1.4.8. Звукоизоляция помещений

Звукоизоляция помещений характеризует уровень проникновения шумов извне и утечку речевой информации из помещения.

Рассмотрим наиболее характерный случай: проникновение звуковых сигналов из одного помещения в другое через смежную перегородку (рис. 1.38).

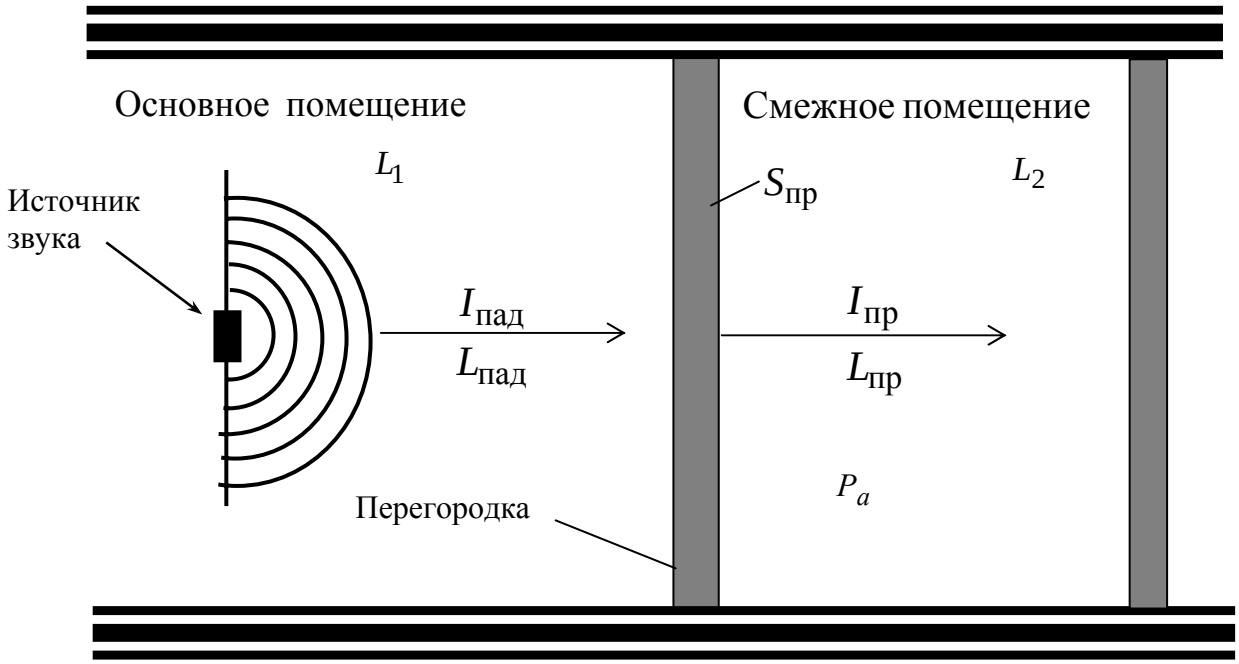


Рис. 1.38. Звукоизоляция помещений

При воздействии звуковых волн с интенсивностью $I_{пад}$ на перегородку больших размеров по сравнению с длиной волны интенсивность волн по другую сторону перегородки $I_{пр}$ при отсутствии отражения звука в другом помещении будет определяться проводимостью перегородки, которая характеризуется коэффициентом звукопроводности

$$\alpha_{пр} = I_{пр} / I_{пад} \qquad (1.91)$$

или звукоизоляцией перегородки

$$Q_{\text{пер}} = 10\lg\frac{1}{\alpha_{\text{пр}}} = 10\lg\frac{I_{\text{пад}}}{I_{\text{пр}}} = L_{\text{пад}} - L_{\text{пр}}, \qquad (1.92)$$

где $L_{\text{пад}}$ и $L_{\text{пр}}$ – уровни интенсивности звуковых волн, падающих на перегородку и прошедших через нее.

Звуковые волны, проникнув в помещение, отражаются от его внутренних поверхностей и увеличивают в нем интенсивность звука.

Можно считать [37], что произведение интенсивности звука $I_{\text{пр}}$, прошедшего через перегородку, на площадь перегородки $S_{\text{пр}}$ будет представлять собой мощность $P_{\text{а}} = I_{\text{пр}} S_{\text{пр}}$, а плотность энергии в помещении

$$\varepsilon_m = \frac{P_{\text{а}}}{c_{\text{зв}}\alpha_{\text{ср}} S} = \frac{I_{\text{пр}} S_{\text{пр}}}{c_{\text{зв}}\alpha_{\text{ср}} S} = \frac{I_{\text{пр}} S_{\text{пр}}}{c_{\text{зв}} A}, \qquad (1.93)$$

где $\alpha_{\text{ср}} S = A$ – общее поглощение ограничивающих поверхностей помещения. Тогда уровень звука в помещении

$$L_2 = 10\lg\frac{\varepsilon_m}{\varepsilon_0} = 10\lg\frac{I_{\text{пр}} S_{\text{пр}}}{\varepsilon_0 c_{\text{зв}}\alpha_{\text{ср}} S}. \qquad (1.94)$$

Так как интенсивность нулевого уровня $\varepsilon_0 c_{\text{зв}} = I_0$, то величина $10\lg(I_{\text{пр}}/I_0) = L_{\text{пр}}$ является уровнем волн, прошедших перегородку. С учетом этих замечаний выражение (1.94) можно записать в виде

$$L_2 = 10\lg\frac{I_{\text{пр}} S_{\text{пр}}}{\varepsilon_0 c_{\text{зв}}\alpha_{\text{ср}} S} = 10\lg\frac{I_{\text{пр}} S_{\text{пр}}}{I_0\alpha_{\text{ср}} S} = 10\lg\frac{I_{\text{пр}}}{I_0} + 10\lg\frac{S_{\text{пр}}}{\alpha_{\text{ср}} S} = L_{\text{пр}} + 10\lg(S_{\text{пр}}/\alpha_{\text{ср}} S). \qquad (1.95)$$

Из выражения (1.95) следует, что составляющая $10\lg(S_{\text{пр}}/\alpha_{\text{ср}} S)$ соответствует приращению интенсивности звука из-за его отражения от ограничивающих смежное помещение поверхностей.

Звукоизоляцией помещения $Q_{\text{из}}$ называют разность между уровнями звука с внешней стороны ограждающей конструкции L_1 и внутри смежного помещения L_2:

$$Q_{\text{из}} = L_1 - L_2 = 10\lg(I_1/I_0) - 10\lg(I_2/I_0) = 10\lg(I_1/I_2), \qquad (1.96)$$

где I_1 и I_2 – интенсивности звука, соответствующие уровням L_1 и L_2.

Учитывая, что уровень интенсивности звука у перегородки со стороны основного помещения $L_1 = L_{\text{пад}}$, а согласно (1.92) $Q_{\text{пер}} = L_{\text{пад}} - L_{\text{пр}}$, откуда следует $L_{\text{пад}} = Q_{\text{пер}} + L_{\text{пр}}$. Тогда, принимая во внимание значение L_2 из выражения (1.95), выражение (1.96) преобразуем к виду

$$Q_{\text{из}} = L_1 - L_2 = L_{\text{пад}} - L_2 = Q_{\text{пер}} + L_{\text{пр}} - L_2 = Q_{\text{пер}} + L_{\text{пр}} - [L_{\text{пр}} + 10\lg(S_{\text{пр}} / \alpha_{\text{ср}} S)] =$$
$$= Q_{\text{пер}} - 10\lg(S_{\text{пр}} / \alpha_{\text{ср}} S). \qquad (1.97)$$

Из (1.97) следует, что звукоизоляция помещения определяется звукоизоляцией ограждающих конструкций с поправкой $10\lg(S_{\text{пр}} / \alpha_{\text{ср}} S)$ на увеличение уровня интенсивности прошедшего звука из-за отражений от внутренних поверхностей смежного помещения. Величина поправки зависит от отношения площади перегородки $S_{\text{пр}}$ к общему поглощению помещения $\alpha_{\text{ср}} S$. В гулком помещении звукоизоляция будет снижаться, а в заглушенных помещениях будет определяться только звукоизоляцией перегородки.

Если полагать, что звуковые волны проникают через состоящую из нескольких участков с разной звукопроводностью сложную перегородку без взаимного влияния, то общая мощность прошедших звуковых волн будет равна сумме мощностей отдельных участков перегородки:

$$P_{\text{а}} = \sum_{(k)} I_{\text{пр}.k} S_{\text{пр}.k},$$

где $I_{\text{пр}.k}$ – поток энергии через единицу k-й поверхности площадью $S_{\text{пр}.k}$.

Прохождение звука через ограждающие конструкции возможно различными путями, в первую очередь через щели и сквозные поры (так называемый воздушный перенос). Через материал перегородок звук проникает из-за продольных колебаний (материальный перенос) поперечных колебаний, схожих с колебаниями мембраны (мембранный перенос). Мембранные колебания в первом приближении можно рассматривать как колебания перегородки как единого целого с коэффициентом звукопроводности, обратно пропорциональным общей массе и с низкой резонансной частотой. С повышением частоты звука звуковая проводимость перегородки пропорционально уменьшается.

При материальном переносе звукопроводимость перегородки зависит от отношения удельных акустических сопротивлений воздуха и материала перегородки, которые от частоты не зависят.

От размеров щелей, пор и т.п., от их расположения и от трения воздуха о поверхности стенок пор зависит эффективность воздушного переноса. Если имеется не менее двух пор, удаленных друг от друга на расстояние больше длины звуковой волны, то в результате дифракции звуковые волны, падающие на перегородку на расстоянии менее половины длины волны от щелей, будут также уходить через щели. Проводимость такой перегородки на высоких частотах будет меньше, чем на низких.

Для снижения проводимости вентиляционных каналов применяют покрытие их звукопоглощающими материалами и акустические фильтры.

Свойства и особенности акустических каналов утечки речевой информации из помещений вытекают из ранее рассмотренных основных положений акустики. По акустическим каналам информация может быть перехвачена с помощью микрофонов или непосредственным прослушиванием.

Наиболее опасными являются технологические окна, короба коммуникаций и вентиляционные конструкции с большой площадью поперечного сечения. Такие конструкции на определенных частотах обладают свойствами акустических волноводов, по которым звук распространяется на значительные расстояния. Особенно опасной ситуация становится, если поперечные размеры коробов сравнимы с длиной звуковых волн.

Также опасными являются звуководы с геометрическими размерами значительно меньшими длины волны. К ним относятся всевозможного вида щели, отверстия, сквозные зазоры в окнах и дверях. Такие звуководы снижают общую звукоизоляцию стены в несколько раз, несмотря на большое затухание в них звуковой волны (до 1…20 дБ/м).

Колебания ограждающих конструкций выделенного помещения, возникающие под действием падающей волны при больших площадях поверхности, являются причиной переизлучения звуковой энергии. При достаточной величине переизлученной звуковой энергии речевая информация может быть перехвачена.

Переизлучение является не единственной причиной утечки речевой информации. Вибрационные колебания строительных конструкций создают один из самых опасных каналов утечки информации – виброакустический канал. Опасность канала определяется тем, что затухание звуковых колебаний в твердых средах (сплошной железобетон, металлические конструкции инженерных коммуникаций, кирпичная кладка и т.п.) характеризуется низким значением в области звуковых частот. Это обстоятельство определяет возможность распространения колебаний на значительные расстояния, превышающие контролируемую зону, где могут быть перехвачены регистрирующей аппаратурой. Перехват информации из выделенного помещения по несущей стене возможен в местах, расположенных через два этажа от помещения.

В некоторых случаях трубы инженерных коммуникаций могут образовать волноводы вибрационных колебаний, распространяющие сигналы на большие расстояния. Условия образования волноводов вибрационных колебаний определяются значительной разницей величин акустических сопротивлений материалов труб и окружающей среды и наличие согласующих элементов между средами, например, батарей отопления.

1.4.9. Акустические каналы утечки речевой информации

1.4.9.1. Микрофоны

Все средства акустической разведки в своей основе используют микрофоны различных типов и назначения. К основным характеристикам микрофонов относятся: чувствительность, частотная характеристика, характеристика направленности и уровень собственного шума [6, 7].

Чувствительность определяется отношением напряжения U на выходе микрофона к звуковому давлению p на его входе при номинальной нагрузке:

$$E = \frac{U}{p} \ . \qquad (1.98)$$

Чувствительность микрофона определяется частотой акустического сигнала, так как от частоты зависит внутреннее сопротивление. Для определения средней чувствительности вводится понятие среднеквадратичного значения в номинальном диапазоне частот.

Чувствительность, выраженная в децибелах относительно величины $1\frac{\text{В}}{\text{Н/м}}$, называется уровнем чувствительности.

Стационарным уровнем чувствительности называется, выраженное в децибелах отношение $U_{\text{н}}$ при номинальной нагрузке $R_{\text{н}}$ при звуковом давлении $1\,\text{Па} = 1\frac{\text{Н}}{\text{м}}$ к напряжению U, соответствующему мощности $p_0 = 1\text{мВт}$. Зависимость уровня чувствительности от частоты называется частотной характеристикой чувствительности.

Характеристика направленности представляет собой зависимость чувствительности микрофона от угла между рабочей осью микрофона (направление, по которому микрофон имеет наибольшую чувствительность) и направлением на источник звука. Эту характеристику определяют для полосы частот. Нормированная характеристика направленности, т.е. зависимость отношения чувствительности E_q, измеренной под углом q, к осевой чувствительности E_0 определяется выражением

$$R(q) = \frac{E_q}{E_0} \qquad (1.99)$$

Большинство микрофонов имеет осевую симметрию. По характеристике направленности микрофоны, используемые для ведения акустической разведки, делятся на направленные (односторонне направленные) и остронаправленные. Графическое представление характеристик направленности называют диаграммой направленности, которую часто представляют в полярных координатах.

Коэффициент направленности G – отношение квадрата осевой чувствительности микрофона в свободном поле E_0 к среднеквадратичной чувствительности по всем радиальным направлениям E_{qs}

$$G = \frac{E_0}{E_{qs}}. \qquad (1.100)$$

Его определяют для полосы частот.

Уровень собственного шума микрофона L, приведённый к акустическому входу, определяют как уровень эквивалентного звукового давления $P_{\text{ш}}$, при воздействии которого на микрофон получилось бы выходное напряжение равное выходному напряжению микрофона $U_{\text{ш}}$, развиваемое им в отсутствии звуковых колебаний:

$$L = 20\lg(p_{\text{ш}} / p_{\text{о}}), \qquad (1.101)$$

где $p_{\text{ш}} = U_{\text{ш}}/E_0$; E_0 – осевая чувствительность; $p_{\text{о}} = 2*10^{-5}$ Па.

Микрофоны по принципу электромеханического преобразования делятся на *электродинамические, электростатические, электромагнитные и релейные*.

Электродинамические микрофоны по конструкции механической системы делятся на *катушечные* (динамические) и *ленточные* [6]. Электростатические делятся на *конденсаторные*, в том числе и электретные, и *пьезомикрофоны*. Электромагнитные делятся на односторонние и дифференциальные. Релейные делятся на угольные и транзисторные.

По акустическим характеристикам микрофоны делятся на приемники давления, приемники градиента давления, комбинированные и групповые.

Особенностью приемника давления является то, что его подвижная механическая система (диафрагма) подвержена воздействию звуковых волн только с одной стороны.

У приемника градиента давления подвижная механическая система открыта для звуковых волн с обеих сторон, поэтому на неё действует разность давлений волн падающих на фронтальную поверхность диафрагмы и огибающей её с тыльной стороны.

Для получения различных форм характеристик направленности обычно комбинируют приемники давления и градиента давления.

Динамический микрофон представляет собой катушку, находящуюся в магнитном поле кольцевого магнита и жестко связанную с диафрагмой.

Конденсаторный микрофон – это конденсатор, у которого один из элементов массивный, а другой – тонкая натяжная мембрана. При колебаниях мембраны емкость конденсатора изменяется, а заряд q остается неизменным (конденсатор в цепи постоянного тока с последовательно включенным большим сопротивлением нагрузки $R_н$ не успевает разряжаться). В результате изменяется напряжение на конденсаторе в соответствии с выражением

$$i = C\frac{du_C}{dt}. \qquad (1.102)$$

Напряжение снимается с сопротивления нагрузки.

В электретном микрофоне поляризующее напряжение образовано предварительной электризацией одного из электродов, изготовляемого из полимеров или керамических поляризующихся материалов. Такой электрод имеет металлическое покрытие, которое является электродом конденсатора, а электрет служит лишь источником поляризующего напряжения. Из-за уменьшения поляризации электрета с течением времени требуется или замена, или повторная поляризация через несколько лет. По характеристикам такой микрофон не отличается от конденсаторного, но не требует источника напряжения.

В пьезомикрофонах используется явление пьезоэффекта. При деформации пластинки из кварца или пьезокерамиков (титан, барий и др.) происходит её поляризация, т.е. концентрация зарядов на плоскостях. Пьезомикрофоны относятся к электростатическому типу микрофонов и не требуют источника питания. Они сходны по свойствам с электретными микрофонами.

1.4.9.2. Направленные микрофоны

Направленные микрофоны предназначены прежде всего для акустического контроля источников звуков на открытом воздухе. В таких ситуациях решающим фактором оказывается удаленность источника звука от направленного микрофона, что приводит к значительному ослаблению уровня контролируемого звукового поля (кроме того, при большой дистанции становится заметным ослабление звука из-за разрушения пространственной когерентности поля вследствие наличия естественных рассеивателей энергии, например средне- и крупномасштабных турбулентностей атмосферы, создающих помехи при ветре) [7].

Так, на дистанции 100 м давление звука ослабляется на величину не менее 40 дБ (по сравнению с дистанцией 1 м), и тогда степень громкости обычного разговора в 60 дБ окажется в точке приема не более 20 дБ. Такое давление существенно меньше не только уровня реальных внешних акустических помех, но и пороговой акустической чувствительности обычных микрофонов.

В отличие от обычных, направленные микрофоны должны иметь [7]:

- Высокую пороговую акустическую чувствительность, чтобы ослабленный звуковой сигнал превышал уровень собственных (в основном тепловых) шумов приемника. Даже при отсутствии внешних акустических помех это является необходимым условием контроля звука на значительном расстоянии от источника.

Виды направленных микрофонов. Существует четыре вида направленных микрофонов [7]:

- параболические;
- плоские акустические фазированные решетки;
- трубчатые, или микрофоны "бегущей" волны;
- градиентные.

Параболический микрофон состоит из отражателя звука параболической формы, в фокусе которого расположен обычный (ненаправленный) микрофон. Отражатель изготавливается как из оптически непрозрачного, так и прозрачного материала.

Величина внешнего диаметра параболического зеркала может находиться в пределах от 200 до 500 мм. Принцип работы этого микрофона поясняется на рис. 1.39.

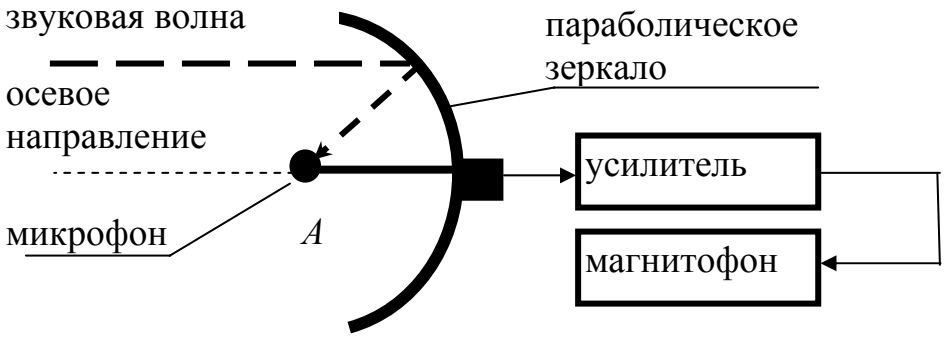


Рис. 1.39. Параболический микрофон

Звуковые волны с осевого направления отражаются от параболического зеркала и суммируются в фазе в фокальной точке *A*. За счет этого эффекта возникает усиление звукового поля. Чем больше диаметр зеркала, тем большим усилением характеризуется микрофон. Если направление волны звука не осевое, то сложение отраженных от различных частей параболического зеркала звуковых волн в точке *A* произойдет со сдвигом по фазе и усиление микрофона будет меньшим. Ослабление тем сильнее, чем больше угол прихода звука по отношению к оси. Параболический микрофон является примером высокочувствительного, но слабонаправленного микрофона.

Плоские фазированные решетки обеспечивают одновременный прием звукового поля в дискретных точках некоторой плоскости, перпендикулярной к направлению на источник звука (рис. 1.40).

Трубчатый микрофон представляет собой звуковод в форме жесткой полой трубки диаметром 10–30 мм со специальными щелевыми отверстиями, размещенными рядами вдоль оси звуковода, с круговой геометрией расположения для каждого из рядов. При приеме звуковой волны с осевого направления будет происходить сложение в фазе сигналов, проникающих в

звуковод через все щелевые отверстия, в силу равенства скоростей осевого распространения звука вне трубки и внутри нее. Когда же звук приходит под некоторым углом к оси микрофона, то это ведет к неравенству длин путей распространения звуковых волн и фазовому рассогласованию, в результате чего снижается чувствительность приема. Обычно длина трубчатого микрофона находится в пределах от 15–230 мм до 1 м. Чем больше его длина, тем сильнее подавляются помехи с боковых и тыльного направлений.

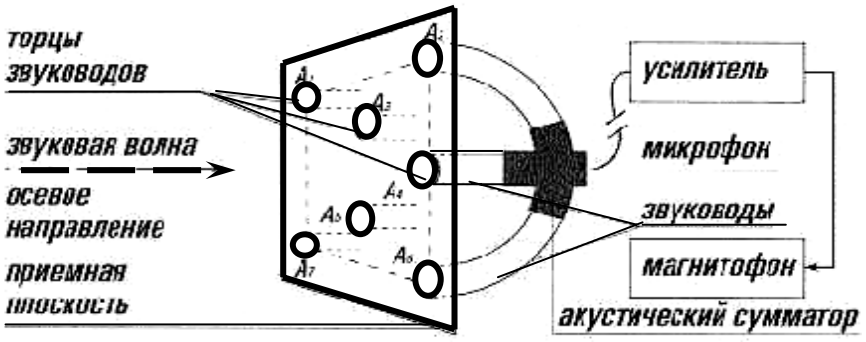


Рис. 1.40. Плоская фазированная решетка

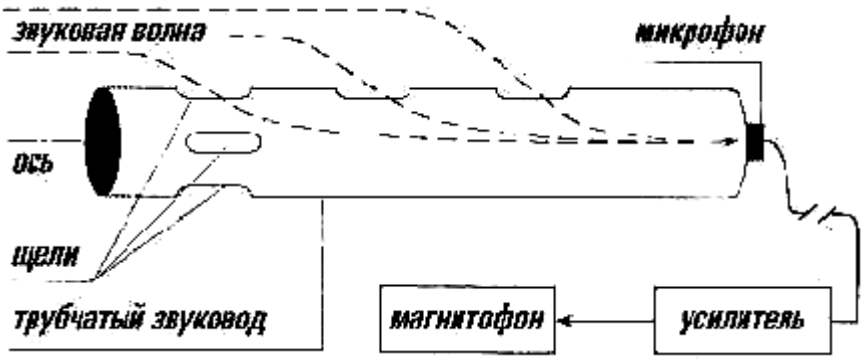


Рис. 1.41. Трубчатый микрофон

Примеры технической реализации направленных микрофонов приведены ниже.

Монокуляр с направленным микрофоном «СУПЕР УХО-100» (рис. 1.42) обеспечивает 8 кратное увеличение [53]. Параболический отражатель способствует созданию узкой диаграммы направленности микрофона. Имеется возможность аудиозаписи на встроенный диктофон в течение 12 сек. Дальность действия микрофона до 100 м. Питание 9 В от батареи типа «Крона». Наушники входят в комплект поставки.

Рис. 1.42. Монокуляр с направленным микрофоном «СУПЕР УХО-100»

Направленный микрофон «Yukon» (рис. 1.43) – это высококачественный профессиональный прибор для прослушивания и записи звуковых сигналов от удаленных объектов [54]. Микрофон имеет штативное гнездо 1/4 дм, которое позволяет установить его на стандартный штатив.

Рис. 1.43. Направленный микрофон «Yukon»

Данный микрофон имеет узкую диаграмму направленности – суперкардиоиду. Изготовленный по новейшей технологии направленный микрофон «Yukon» является высокочувствительным конденсаторным микрофоном, позволяющим услышать звуки на расстоянии до 100 м.

Микрофон имеет автономное питание, обеспечивающее непрерывную работу в течение 300 ч. Эффективная ветрозащита позволяет значительно снизить фон от воздушных потоков.

В приборе ночного видения с направленным микрофоном NVS 2,5×42 (рис. 1.44) впервые реализована идея одновременного визуального и акустического контроля в условиях естественной ночной освещенности за объектами, расположенными на значительном удалении от наблюдателя [55].

В приборе ночного видения используется оптическая схема, базирующаяся на электронно-оптических преобразователях нулевого поколения. Благодаря оптимально рассчитанной кратности (2,5) и светосиле, прибор обеспечивает высокое качество изображения. Наличие фотоадаптера позволяет проводить фото- и видео съемку в ночных условиях. Мощный ИК-осветитель дает возможность вести наблюдение в условиях полной темноты.

Рис. 1.44. Направленный микрофон с прибором ночного видения NVS 2,5×42

С помощью направленного микрофона можно осуществлять прослушивание и запись различных звуковых сигналов на расстоянии до 100 м.

1.4.9.3. Проводные системы, портативные диктофоны и электронные стетоскопы

Средства акустической разведки выбираются в зависимости от возможности доступа в контролируемые места.

Микрофоны всех типов имеют диапазон чувствительности от 6 до 10 мВ/Па и в состоянии регистрировать голос человека нормальной громкости на расстоянии 10–15 м, а некоторые образцы – до 20 м, в частотном диапазоне 100 Гц – 20 кГц.

Если имеется возможность постоянного проникновения в контролируемые помещения, в нем заранее могут быть установлены миниатюрные микрофоны, линии передачи сигналов которых выводятся в специальное помещение, где находится злоумышленник и установлена регистрирующая аппаратура. Длина линии передачи сигнала может достигать 5000 м. Такие системы называются проводными системами [1].

Для обеспечения скрытности микрофонов последние выпускаются в сверхминиатюрном исполнении (диаметр менее 2,5 мм) и камуфлируются под различные предметы.

Для повышения качества перехваченных разговоров микрофоны устанавливаются возможно ближе к местам проводимых разговоров, а улучшение чувствительности может быть обеспечено подключением микрофонов к предусилителям.

В качестве регистрирующей аппаратуры используются магнитофоны и диктофоны с длительным временем записи (до 16 ч). Для улучшения качества записи и скрытности всё чаще используются цифровые магнитофоны. Цифровой бескинематический магнитофон «U-7102» показан на рис. 1.45. В аппарате для преобразования речевого сигнала в цифровой поток используется кодер V-16 [56]. Алгоритм обеспечивает длительное время записи информации без применения программного сжатия и позволяет получать высокое качество речевой информации в сложных акустических условиях. Магнитофон обеспечивает высокое качество записи информации при работе систем подавления диктофонов и в условиях постановки целенаправленных акустических помех.

Рис. 1.45. Цифровой бескинематический магнитофон «U-7102»

- возможность программного конвертирования записанной информации в стандартный WAV-файл;
- программное стирание записанной информации.

Блок воспроизведения некоторых магнитофонов позволяет подключение к компьютеру. Для управления воспроизведением применяют программное обеспечение, которое позволяет:

- моментально получить доступ к любому ранее записанному фрагменту в выбранном для прослушивания файле;
- отсортировать записанные разговоры по различным признакам (время начала, длительность, номер канала с одним из микрофонов подслушивания);
- выделять и копировать в новый файл как разговоры полностью, так и фрагменты из них по выбору и в любом порядке;
- переписывать созданные файлы фрагментов на другие носители;

Эквалайзеры представляют собой специальные устройства с набором различных фильтров: фильтров верхних и нижних частот, полосовых, основных, чебышевских и др. Эти фильтры включаются по определенной программе в зависимости от характера искажений сигнала и помех и повышают разборчивость речи.

Наряду с эквалайзерами для повышения разборчивости речи используются специальные программно-аппаратные комплексы. Обычно в состав подобных комплексов входят:

- устройство ввода/вывода речевых сигналов, включающее АЦП и ЦАП;
- плата специализированного сигнального процессора, предназначенного для реализации в реальном масштабе времени процедур обработки речевых сигналов, в частности шумоподавления;
- пульт управления;
- компьютер;
- программное обеспечение и другие средства.

Если не удается проникнуть в контролируемое помещение, но имеется возможность проникновения в соседнее помещение, то для сбора речевой информации используются электронные стетоскопы, преобразующие акустические колебания в твердых телах (стенах, потолках, полах, трубах) в электрические сигналы. Чувствительным элементам электронных стетоскопов является контактный микрофон (чаще всего на основе пьезоэлемента), соединенный с усилителем. Стетоскоп представляет собой вибродатчик, усилитель и головные телефоны. Размеры датчика, на примере устройства DTI, составляют 2,2×8 см. С помощью подобных устройств можно осуществлять прослушивание разговоров через стены толщиной до 1 м. Стетоскоп может оснащаться проводным, радио или другим каналом передачи информации. Достоинством стетоскопа является трудность его обнаружения при установке в соседних помещениях.

Имеются стетоскопы, у которых чувствительный элемент, усилитель и радиопередатчик имеют общий корпус. Примером такого устройства является стетоскоп АД-50. Этот компактный стетоскоп позволяет не только прослушивать разговоры через стены, оконные рамы, двери, но и передавать информацию по радиоканалу. Он имеет высокую чувствительность и

обеспечивает хорошую разборчивость речевого сигнала. Его несущая частота составляет 470 МГц, дальность передачи – до 100 м.

На рис. 1.46 показан стереофонический стетоскоп СС 021, предназначенный для анализа виброакустической защиты строительных конструкций. Датчики стетоскопа имеют чувствительность не хуже 10^{-5} g [57].

Рис. 1.46. Стетоскоп стереофонический СС 021

Современные электронные стетоскопы имеют коэффициент усиления до 30000 и способны фиксировать слабые звуковые колебания (шорохи, тиканье часов) через бетонные стены толщиной 50–100 см [6].

1.4.9.4. Радиомикрофоны

Принцип действия радиозакладок микрофонного типа основан на преобразовании акустических сигналов с помощью микрофона в электрические сигналы и передачи их по радиоканалу на приемное устройство. Такие подслушивающие устройства получили наибольшее распространение благодаря простоте исполнения и дешевизне. В качестве источника питания могут служить автономные источники питания, электрическая и телефонная сети.

- микрофон, воспринимающий акустические колебания разговаривающих лиц и превращающий их в электрические сигналы;
- радиопередатчик, воспринимающий электрические сигналы от микрофона и передающий их по радиолинии на приемник, позволяющий злоумышленнику воспринимать содержание переговоров;
- источник питания радиопередатчика, определяющий продолжительность непрерывной работы радиозакладок.

Микрофон определяет зону акустической чувствительности (до 20–30 м), радиопередатчик – дальность действия радиолинии. Важными параметрами с точки зрения дальности действия для передатчика являются мощность, стабильность несущей частоты, диапазон частот, вид модуляции.

По конструктивному исполнению радиозакладки могут быть простыми, работающими как обычные передатчики с амплитудной или частотной модуляцией. В то же время радиозакладки могут быть и весьма сложными: иметь в своем составе устройства дистанционного управления, автоматиче-

ского включения при определенных условиях, системы накопления информации и передачи ее короткими сериями на повышенных скоростях и т.д.

Наличие такого большого количества моделей радиомикрофонов объясняется тем, что в различных ситуациях требуется определенная модель.

Радиозакладки, устанавливаемые в телефонную линию, используют её и в качестве источника питания и в качестве антенны. Некоторые позволяют прослушивать только телефонные разговоры, а некоторые ещё и разговоры в помещении, где установлен телефонный аппарат. При разговоре акустические волны воздействуют на телефонный капсюль и он передает сигналы по сети, даже если трубка положена. При поднятии трубки закладка переходит в режим прослушивания телефонного разговора. Такие закладки удобны тем, что можно слушать, например, и телефон и квартиру, даже не проникая в неё, достаточно подключить такую закладку к телефонной линии в подъезде. Подключаются телефонные закладки к линии по параллельной схеме.

Так как питается такая закладка от телефонной линии, то время её работы практически не ограничено.

1.4.9.5. Гидроакустические датчики

Звуковые волны распространяются в воде с очень небольшим затуханием. Этот принцип можно применять для их регистрации, используя жидкость, находящуюся в системах водоснабжения и канализации. Такую информацию можно получить в пределах здания, но радиус прослушивания будет очень сильно зависеть от уровня шумов, особенно в водопроводе. Ещё более эффективным будет использование гидроакустического передатчика, установленного в батарее прослушиваемого помещения.

1.4.9.6. СВЧ- и ИК-передатчики

Для повышения скрытности передачи речевой информации используется инфракрасный канал. В качестве передатчика звука от микрофона используется полупроводниковый лазер. В качестве примера приведем устройство TRM-1830. Дальность действия днем составляет 150 м, ночью – 400 м, время непрерывной работы – 20 ч. Габариты не превышают 26×22×20 мм. К недостаткам подобной системы можно отнести необходимость прямой видимости между передатчиком и приемником и влияние помех на качество передачи сигналов.

Повысить скрытность получения информации можно также с помощью использования канала СВЧ в диапазоне более 10 ГГц. Передатчик, выполненный на диоде Ганна, может иметь очень небольшие габариты.

К преимуществам такой системы можно отнести отсутствие помех, простоту и отсутствие в настоящее время эффективных средств контроля.

К недостаткам следует отнести необходимость прямой видимости, хотя и в меньшей степени, так как СВЧ-сигнал может все-таки огибать небольшие препятствия и проходит хотя и с ослаблением сквозь тонкие диэлектрики, например, шторы на окнах.

1.4.10. Виброакустические технические каналы утечки речевой информации

Перехват акустических сигналов по виброакустическим техническим каналам возможен:

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

1.4.11. Акустоэлектрические каналы утечки речевой информации

Перехват акустических колебаний возможен:

- через ВТСС, обладающих «микрофонным эффектом», путем подключения к их соединительным линиям;
- через ВТСС путем «высокочастотного навязывания».

1.4.12. Оптико-электронный технический канал утечки речевой информации

Оптико-электронный технический канал утечки информации образуется путем облучения лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, картин, зеркал).

Схема простейшего лазерного микрофона показана на рис. 1.47. Звуковая волна, генерируемая источником акустического сигнала, падает на границу раздела воздух-стекло со стороны помещения и создает вибрацию (отклонения поверхности стекла от исходного положения). Эти отклонения вызывают дифракцию света, отражающегося от внешней стороны стекла.

Если размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в составе различных компонент отраженного света будет доминировать дифракционный пучок нулевого порядка. В этом случае, во-первых, фаза световой волны оказывается промодулированной по времени с частотой звука и однородной по сечению пучка, а

во-вторых, пучок «качается» с частотой звука вокруг направления зеркального отражения.

Отраженное лазерное излучение принимается от сплиттера чувствительным приемником лазерного излучения (детектором). Применение сплиттера (делителя пучка) позволяет свести падающий и отражённый луч в одну точку. При демодуляции отраженного лазерного излучения выделяется речевая информация.

Лазер и приемник образуют сложную лазерную акустическую локационную систему («лазерный микрофон»), работающую в ближнем инфракрасном диапазоне волн.

Реально лазер, сплиттер и детектор могут быть совмещены в одном устройстве.

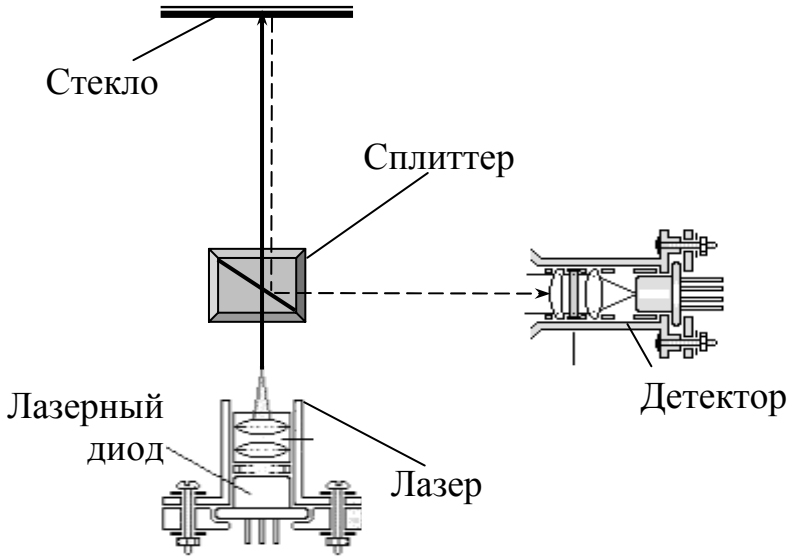


Рис. 1.47. Схема простейшего лазерного микрофона

В открытых публикациях сообщается, что, например, система SIPE LASER 3-DA SUPER производства США использует в качестве источника излучения гелий-неоновый лазер. Наведение прибора на объект осуществляется с помощью телескопического визира, а съем речевой информации с оконных рам с двойным остеклением обеспечивается с расстояния до 250 м с хорошим качеством. Другое лазерное устройство HPO150 фирмы HEWLETT PACKARD обеспечивает регистрацию разговоров, ведущихся в помещениях, на дальности до 1000 м.

Качество принимаемой информации зависит от следующих факторов:

- параметров используемого лазера (длина волны, мощность, когерентность и т. д.);
- параметров фотоприемника (чувствительность и избирательность фотодетектора, вид обработки принимаемого сигнала и т.д.);
- параметров атмосферы (рассеяние, поглощение, турбулентность, уровень фоновой засветки и т.д.);

• качества обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды);

• уровня фоновых акустических шумов;

• уровня перехваченного речевого сигнала.

1.4.13. Параметрические технические каналы утечки речевой информации

Перехват акустических сигналов в параметрических технических каналах утечки информации возможен:

• путем приема и детектирования электромагнитных излучений (ЭМИ) на частотах ВЧ генераторов ТСПИ и ВТСС, модулированных информационным сигналом;

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

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

Примером полуактивного закладного устройства может служить аудио-транспондер (рис. 1.48). Он начинает работать только тогда, когда происходит его облучение высокочастотным зондирующим сигналом. Транспондер трудно обнаружить, так как он может быть вмонтирован в стену.

Приемник транспондера принимает зондирующий сигнал и подает его на узкополосный частотный модулятор. Модулирующим является сигнал, поступающий непосредственно от микрофона или от микрофонного усилителя. Модулированный высокочастотный сигнал переизлучается со смеще-

нием по частоте относительно опорной. Переизлученный сигнал принимается приемником, в котором осуществляется его демодуляция.

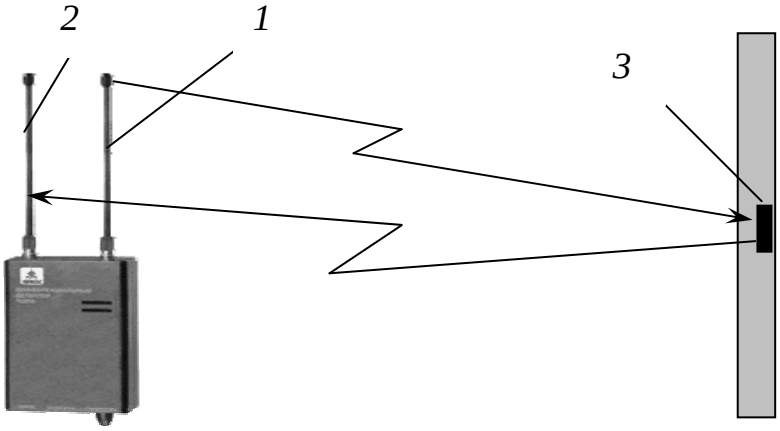


Рис. 1.48. Схема аудио-транспондера: *1* – антенна облучающего передатчика; *2* – антенна приемника; *3* – полуактивная радиозакладка в стене

Из-за отсутствия специального источника питания время работы транспондера не ограничено.

1.5. Технические каналы утечки видовой информации

1.5.1. Способы скрытого видеонаблюдения и съемки

Визуальное наблюдение является самым давним и очень эффективным методом сбора информации. Как известно, высокий уровень охраны субъекта или объекта предполагает значительное насыщение пространства вокруг охраняемого самыми разнообразными техническими средствами и многочисленными сотрудниками охраны. Данное обстоятельство осложняет доступ к объекту и получение информации о деятельности физических лиц. Поэтому для выявления интересующих подробностей в 99% случаев из ста применяется разнообразная оптика [4].

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

Для получения информации широко используется скрытая фото- и видеосъемка.

В настоящее время для сбора информации могут использоваться миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры. На рис. 1.49 показана одна из микрофотокамер – закамуфлированная цифровая микрофотокамера Minox DD1 [49].

Рис. 1.49. Закамуфлированная цифровая микрофотокамера Minox DD1

Фото- и видеокамеры бывают:

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

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

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

Спецслужбы давно и широко применяют различные оптические приборы для скрытного наблюдения и регистрации информации в дневных и ночных условиях при любой погоде. Для видеонаблюдения в дневное время применяются традиционные оптические приборы: бинокли, монокуляры, подзорные трубы, телескопы и др. На рис. 1.50 показаны самые популярные модели зрительных труб фирмы «Bushnell» – «Sentry 18-36×50» [58] и «Spacemaster 20-45×60» [59]. Все линзы и призмы этих труб имеют многослойное просветляющее покрытие, которое обеспечивает хорошую светопередачу и яркое, насыщенное изображение. Линзы труб защищены от дождевых капель и не запотевают ни при каких условиях.

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

Для ведения разведки ночью находят применение специальные телевизионные камеры (рис. 1.51), работающие при низком уровне освещённости, приборы ночного видения (ПНВ) и тепловизионные приборы (ТПВ).

На практике наиболее широко применяются приборы на основе оптикоэлектронных приборов (ОЭП) второго поколения. Такие приборы со-

держат микроканальную пластинку, представляющую собой диск с большим числом микроскопических каналов. Каждый канал является миниатюрным усилителем вторичной эмиссии электронов, испускаемых катодом ОЭП. Приборы обеспечивают возможность регистрации изображения на фото- и видеокамеры. Они обладают высоким усилением (до 50000), устойчивостью к засветкам, например фар автомашин, равномерным по полю разрешением и небольшими габаритами. Принцип их действия основан на приёме отражённого местными предметами оптического ИК-излучения и многократного его усиления и преобразования в видимое изображение [22].

а *б*

Рис. 1.50. Зрительные трубы «Bushnell» – «Sentry 18-36×50» (*а*) и «Spacemaster 20-45×60» (*б*)

Рис. 1.51. Видеокамеры Pelco

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

Комплект маскирования видеоизображения «VideoLock» (рис. 1.52) предназначен для маскирования видеоизображения при передаче его по проводным или радиоканалам [60]. В комплекте применены новейшие цифровые технологии для передачи видеоизображения по проводным и радиоканалам.

Комплект характеризуется следующими свойствами:

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

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

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

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

В последнее время появились тепловизоры, работающие при комнатной температуре (рис. 1.53) [61].

Своевременное выявление и обнаружение средств оптического наблюдения становится важной задачей при проведении как профилактических, так и специальных защитных и охранных мероприятий. Своевременное обнаружение несанкционированного наблюдения позволяет установить цель его проведения и определить потенциальную угрозу факта наблюдения.

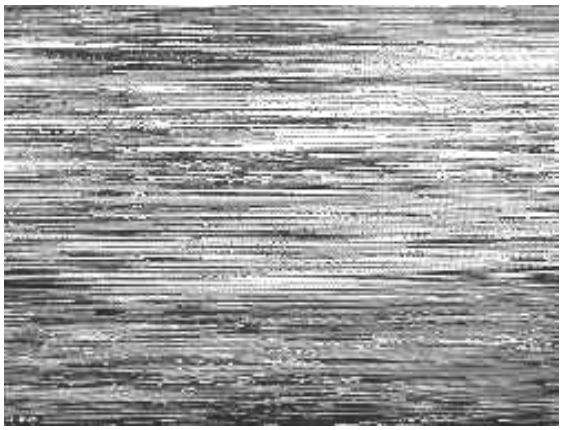
В настоящее время наблюдается значительный рост применения подвижных видеозаписывающих систем в основном двух типов:

• на основе камкодеров (видеокамеры со встроенным портативным видеомагнитофоном);

• на основе кассетных видеомагнитофонов настольного типа и миниатюрных видеокамер на приборах с зарядовой связью (ПЗС).

Кодер

Декодер



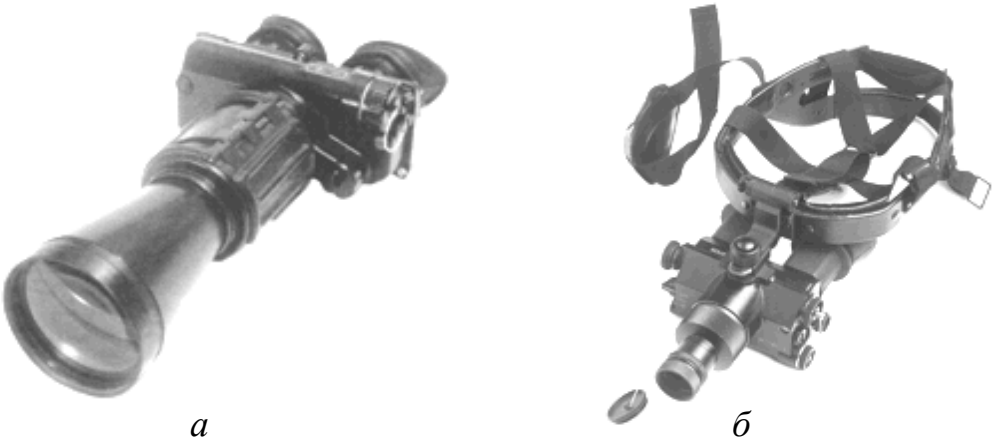
Маскированное изображение

Демаскированное изображение

Рис. 1.52. Комплект маскирования видеоизображения «VideoLock»

Рис. 1.53. Тепловизор ThermaCAM P640
с неохлаждаемым микроболометром
и со встроенной цифровой видеокамерой

В системах первого типа применяются специально модифицированные компактные камкодеры с записью на 8-мм пленку или стандартную пленку для бытовых видеомагнитофонов. Камкодерные системы находят широкое применение благодаря их универсальности и меньшей стоимости технического обслуживания по сравнению с видеомагнитофонными системами. Основное их преимущество состоит в том, что их можно выносить из автомобиля для видеозаписей событий на месте преступления, или происшествия. Время записи находится в пределах от 20 мин до 2 ч, что достаточно для регистрации событий.



а *б*

Рис. 1.54. Бинокль-псевдобинокуляр «1ПН-94» (*а*)
и очки ночного видения «1ПН74» (*б*)

Технические характеристики некоторых перечисленных устройств приведены в [21].

Классическим примером многообразия однородных форм очков ночного видения (ОНВ) можно считать модели «1ПН74» и «1ПН-94» (рис. 1.54, *а* и рис. 1.54, *б*), построенные по псевдобинокулярной схеме. Подобные приборы крепятся на голове оператора на специальных масках для обеспечения движения и ориентирования на местности в ночное время, скрытного наблюдения объектов, выполнения различного рода инженерно-технических работ, управления транспортными средствами по пересечённой местности без использования источников видимого света в ночное время.

Схема 1ПН74 показана на рис. 1.55. ОНВ содержат общий корпус *1*, окуляр *2*, оборачивающий объектив *3*, зеркало *4*, коллиматор с призмой *5*, корпус собственно ОНВ *6*, инфракрасная подсветка *7*, электронно-оптический преобразователь *8*, корпус объектива *9*, объектив *10*, крышка объектива *11*.

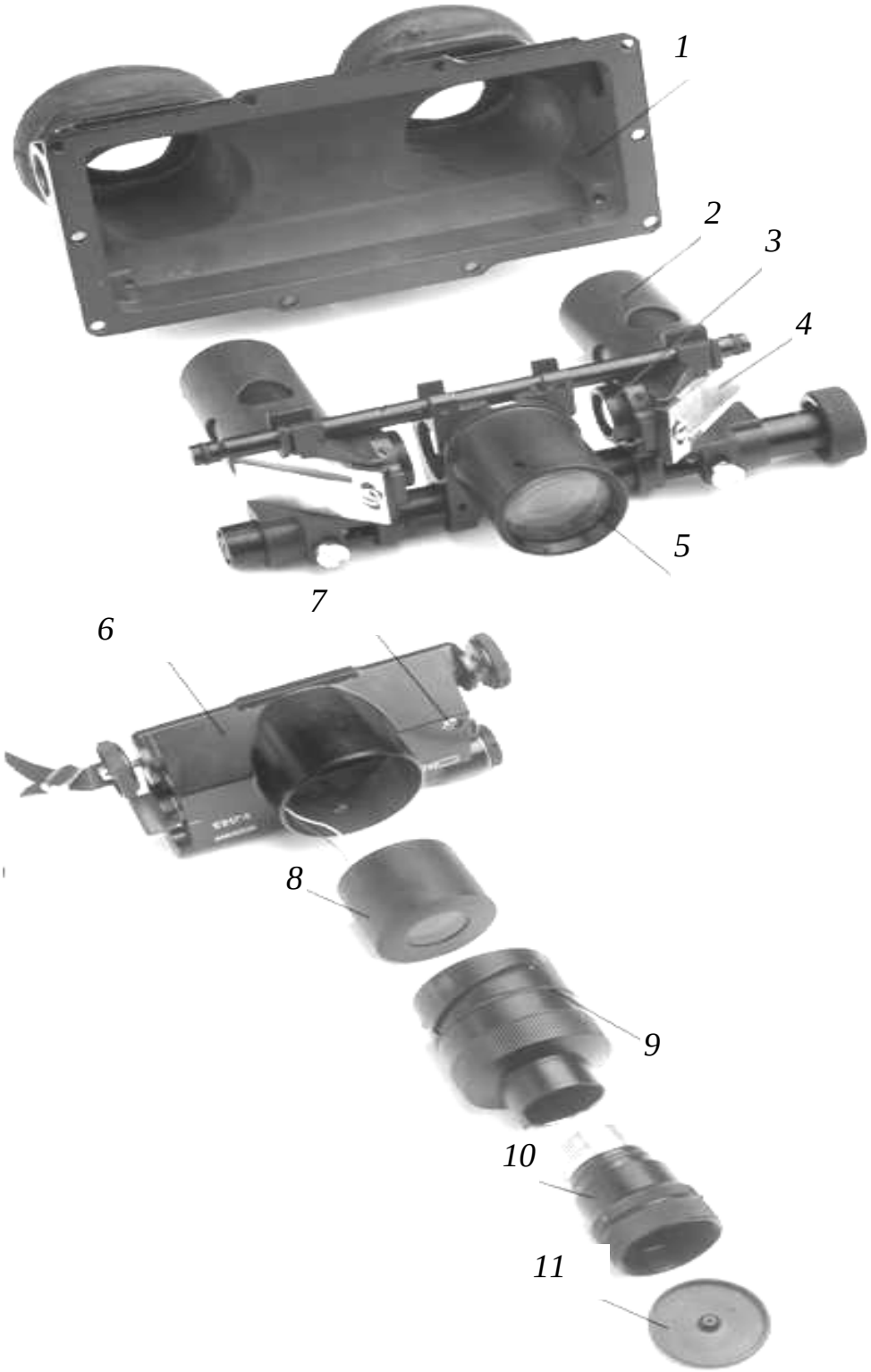


Рис. 1.55. Схема 1ПН74

Вопросы для самопроверки

1. Назовите объекты защиты информации.
2. Что называют техническими средствами приёма, обработки и хранения информации (ТСПИ)?
3. Приведите определение вспомогательных технических средств и систем (ВТСС).
4. Приведите определение объекта *ТСПИ*.
5. Приведите определение *контролируемой зоны*.
6. Что понимают под *посторонними проводниками?*
7. Приведите определение *опасной зоны*.
8. Приведите определение *опасной зоны 1*.
9. Приведите определение *случайной антенны*.
10. Назовите типы случайных антенн.
11. Приведите определение случайной сосредоточенной антенны.
12. Приведите определение случайной распределенной антенны.
13. Что понимают под техническим каналом утечки информации (ТКУИ)?
14. Какие составляющие содержит технический канал утечки информации?
15. Назовите основные группы технических каналов утачки информации.
16. Перечислите каналы утечки информации, обрабатываемой ТСПИ.
17. Перечислите каналы утечки информации при передаче ее по каналам связи.
18. Перечислите каналы утечки речевой информации.
19. Перечислите каналы утечки видовой информации.
20. Приведите определение электромагнитных каналов утечки информации.
21. Какими составляющими характеризуется электромагнитное поле побочных электромагнитных излучений?
22. Какие уравнения используются для расчета электромагнитного поля?
23. Что представляет собой элементарный излучатель?
24. Какими бывают элементарные излучатели?
25. Чему соответствует электрический излучатель?
26. Чем характерна ближняя зона излучения электромагнитного поля?
27. Чему равен фазовый сдвиг между составляющими напряженности магнитного поля H и напряженности электрического поля E электрического излучателя в ближней зоне?
28. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в ближней зоне?

30. В каких границах расолагается дальняя зона электромагнитного поля?

31. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в дальней зоне?

32. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля, создаваемого магнитным диполем в ближней зоне?

33. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля, создаваемого магнитным диполем в дальней зоне?

34. Назовите электромагнитные каналы утечки информации ТСПИ.

35. За счет чего образуются электрические каналы утечки информации?

36. Каким образом создается параметрический канал утечки информации?

37. Перечислите виды паразитных связей в линиях передачи информации.

38. Физические явления, вызывающие емкостные и индуктивные паразитные связи.

39. Как образуется электрический канал утечки информации при ее передаче по линиям связи?

40. Методы контроля и прослушивания телефонных каналов связи.

41. В чем смысл способа прослушивания телефона методом высокочастотной накачки?

42. Определение звукового поля.

43. Определение звукового луча.

44. Определение понятия фронта звуковой волны.

45. Определение понятия звукового давления.

46. Как определяется звуковая мощность? Приведите определение скорости звуковых колебаний.

47. Как определяется звуковая мощность?

48. Приведите определение интенсивности (силы) звука.

48. Приведите определение *плотности звуковой энергии* ε.

2. ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОБЪЕКТОВ

2.1. Общие положения

Под демаскирующим признаком понимается свойство объекта отличаться по каким-либо характеристикам от других объектов. Отличительные характеристики могут иметь количественную или качественную оценку. Технический демаскирующий признак объекта – характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем. Таким образом, доступ к информации может быть осуществлен путем анализа демаскирующих признаков, являющимися по существу своеобразными каналами утечки информации. Носителями демаскирующих признаков являются прямым образом связанные с ними физические поля.

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

Различают демаскирующие признаки:

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

Технические демаскирующие признаки можно разделить на два класса:

- прямые демаскирующие признаки – признаки, связанные с функционированием объекта защиты и проявляющиеся через их физические поля (электромагнитные, акустические, радиационные и т.п.), отличающиеся по уровню на фоне физических полей окружающей среды, не связанных с защищаемой информацией;
- косвенные демаскирующие признаки – признаки, в основе которых лежат последствия изменения окружающей среды как результат функционирования объекта (визуально-оптические признаки деятельности, геометрические размеры, контрастность освещенности, следы производственной деятельности и функционирования и т.п.) [5].

Показатель эффективности защиты информации – параметр технического демаскирующего признака объекта защиты, по отношению к которому устанавливаются нормы по эффективности защиты информации.

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

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

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

2.2. Демаскирующие признаки объектов

К демаскирующим признакам объектов относятся:

– признаки деятельности: движение транспортных машин, звуки, огни, вспышки, дым, пыль;

– способность отражать и испускать различные излучения (электромагнитные, инфракрасные, тепловые), улавливаемые специальными приборами;

– следы деятельности: тропы и дороги, остатки производственных материалов, бытовой мусор и т.д.;

– характерные очертания (форма), размеры и особенности расположения объектов;

– цвет поверхности объектов, а в некоторых случаях и блеск ее (блеск стекол, отблеск металла);

– тени, падающие от объектов, а также тени на поверхности самих объектов.

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

Обнаружение объекта производится по его демаскирующим признакам, которые делятся на три группы: видовые, признаки деятельности и расположения.

К видовым демаскирующим признакам относятся физические свойства объекта (способность отражать излучение оптического и радиолокационного диапазонов волн, излучать энергию в тепловом диапазоне) и геометрические свойства (форма, размер объекта и его отдельных деталей).

Демаскирующие признаки деятельности проявляются в результате действий объекта (перемещение, изменение окружающей среды и др.).

Признаки расположения характеризуются положением объектов относительно местных предметов.

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

2.3. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра

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

Контраст по яркости K определяется как [5]

$$K = \frac{B_{\max} - B_{\min}}{B_{\max}} = 1 - \frac{B_{\min}}{B_{\max}}, \qquad (2.1)$$

где $B_{\min}$ и $B_{\max}$ – минимальная и максимальная яркости поверхностей объекта и фона.

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

$K \leq 0{,}2$ (20%) – незаметный контраст;

$K = 0{,}2–0{,}3$ – малозаметный контраст;

K = 0,3–0,6 – заметный контраст;

$K \geq 0{,}5$ – резкозаметный контраст.

Яркость поверхности предметов зависит от освещенности E, с увеличением которой она пропорционально возрастает. Освещенность в дневное время определяется как [5]

$$E = E_{\text{пр}} + E_{\text{р}}, \tag{2.2}$$

где $E_{\text{пр}}$ – освещенность прямыми солнечными лучами; $E_{\text{р}}$ – освещенность рассеянным светом небосвода. Освещенности зависят от погодных условий, ориентации объектов по отношению к солнцу и других условий. Освещенность прямыми солнечными лучами $E_{\text{пр}}$ наклонной поверхности зависит от косинуса угла падения лучей α.

Кроме освещенности на яркость предметов влияют и их отражающие свойства. В зависимости от свойств поверхности отражение может быть зеркальным (направленным), диффузным (рассеянным) или смешанным. Зеркальное отражение характерно только для гладких поверхностей с малыми размерами неровностей по сравнению с длиной волны. При солнечном освещении такие поверхности дают яркие блики, которые хорошо наблюдаются на большой дальности. Яркость B таких поверхностей определяется как

$$B = \rho B_{\text{ист}}, \tag{2.3}$$

где ρ – коэффициент отражения поверхности; $B_{\text{ист}}$ – яркость источника освещения.

При диффузном отражении отраженная энергия равномерно распределяется в пределах полусферы над точкой отражения. Такое отражение характерно для матовых шероховатых поверхностей. Показателем их отражающих свойств является коэффициент яркости r, представляющий собой отношение яркости поверхности в данном направлении к яркости матовой поверхности при полном отражении падающих на нее лучей:

$$r = \frac{B}{B_0}, \tag{2.4}$$

где B – яркость поверхности в данном направлении; B_0 – яркость одинаково с ней освещенной матовой поверхности полностью отражающей падающий на нее световой поток.

Яркость идеально белой матовой поверхности определяется только значением освещенности E;

$$B_0 = \frac{E}{\pi}, \tag{2.5}$$

следовательно

$$B = rB_0 = \frac{rE}{\pi}. \tag{2.6}$$

При смешанном, т.е. диффузно-зеркальном отражении энергия в полусфере распределена не равномерно. Яркость поверхности $B_{\alpha\beta}$ в этом случае зависит как от направления облучения под углом β, так и от направления наблюдения α:

$$B_{\alpha\beta} = \frac{r_{\alpha\beta} E}{\pi}. \qquad (2.7)$$

Для оценки распределения яркости поверхности в различных направлениях при смешанном отражении также используется коэффициент яркости, который является функцией длины волны, т.е. зависит от спектрального состава падающих лучей и отражающих свойств поверхности в различных участках спектра. Характеристикой отражения при данной длине волны служит спектральный коэффициент яркости r_λ, который определяется отношением эффективной яркости b_λ поверхности к ее яркости при полном отражении энергии облучения $b_{0\lambda}$ монохроматическим потоком с длиной волны λ:

$$r_\lambda = \frac{b_\lambda}{b_{0\lambda}}. \qquad (2.8)$$

Чем меньше различие в спектральных характеристиках поверхностей, тем меньше контраст между ними и тем труднее обнаружить объект.

Величину спектральной яркости освещенной поверхности можно определить по формуле (1.16), заменив соответствующие величины на спектральные.

Видимость объекта зависит также от расстояния. По мере удаления объекта видимость ухудшается. Это обусловлено ослаблением потока при прохождении сквозь атмосферу за счет спектрального поглощения его слоем воздуха, что приводит к уменьшению яркости объекта и фона. Одновременно солнечные лучи, проходя через атмосферу, переотражаются от мельчайших частиц, образуя световоздушную дымку. Таким образом, спектральная (эффективная) яркость поверхности объекта состоит из двух слагаемых: спектральной яркости объекта, наблюдаемого сквозь атмосферу без учета влияния дымки, и яркости вуалирующей световоздушной дымки. Кроме того цветовой контраст между объектом и фоном является дополнительным демаскирующим признаком, позволяющим улучшить видимость объектов. При цветовом соответствии тонов объекта и фона контраст продолжает существовать, так как остается различие в тональной насыщенности поверхности объекта и элементов фона.

В зависимости от вида технических средств разведки, с помощью которых и выявляются демаскирующие признаки объектов, их можно разделить на видовые и радиоразведывательные.

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

К прямым демаскирующим признакам объектов в видимом диапазоне электромагнитного спектра относятся: форма, размер, тон или цвет, структура, текстура и тень объектов. При этом форма изображения объекта является основным признаком. Размер изображения зависит от масштаба фотоснимка и в меньшей степени является информативным, поскольку требует сравнения с некоторым эталоном. Структура изображения объекта является сложным демаскирующим признаком, содержащим в себе группу прямых признаков разнородных деталей изображения местности. Этот признак мало зависит от условий съемки, поэтому наиболее устойчив. Тени объектов подразделяют на собственные (лежащие на объекте с теневой стороны) и падающие (отбрасываемые объектом на окружающую поверхность) [5]. Собственные тени хорошо подчеркивают пространственные формы объекта, а падающие тени способствуют определению не только формы, но и размеров объекта.

Косвенные демаскирующие признаки дополняют некоторые характеристики объектов, не входящие в состав прямых признаков. Так, например, невидимый тоннель можно определить на фотоснимке по разрыву дорожного полотна на определенном участке. К косвенным демаскирующим признакам чаще всего относятся результаты человеческой деятельности на объектах, характерные для определенных типов объектов, а также определенные взаимосвязи совокупности разнородных объектов вплоть до влияния одних объектов на другие.

2.4. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра

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

Обнаружение цели возможно за счет различий в тепловой излучательной способности объекта и фона. Каждый предмет при температуре, отличной от абсолютного нуля, испускает электромагнитное излучение, называемое тепловым. Излучение тел зависит от их температуры и излучательной способности, которые можно характеризовать эффективной температурой тела. Собственное тепловое излучение нагретых тел связано с понятием абсолютно черного тела, поглощающего все падающие на него излучения во всем спектре. Распределение интенсивности излучения по спектру для абсолютно черных тел подчиняется закону Планка [5]

$$B_\lambda^0 = C_1 \lambda^{-5} (e^{\frac{C_2}{\lambda T}} - 1)^{-1}, \qquad (2.9)$$

где B_λ^0 (Вт×см$^{-2}$×ср$^{-1}$×мкм$^{-1}$) – спектральная яркость излучения при температуре T° К; λ (мкм) – длина волны; $C_1 = 1{,}19 \cdot 10^4$ (Вт×мкм^{4}см$^{-2}$×ср$^{-1}$) – коэффициент; $C_2 = 1{,}44 \cdot 10^4$ (мкм×град) – коэффициент.

Максимальное значение спектральной яркости излучения наблюдается на длине волны $\lambda_{макс}$, определяемой по закону Вина:

$$\lambda_{макс} = \frac{2896}{T} \quad (мкм), \qquad (2.10)$$

где T – абсолютная температура тела по Кельвину.

Реальные объекты излучают меньше энергии, чем абсолютно черное тело. Спектральную яркость излучения B_λ реальных объектов можно определить по формуле

$$B_\lambda = \varepsilon_\lambda B_\lambda^0, \qquad (2.11)$$

где ε_λ – коэффициент излучения поверхности объекта (степень черноты).

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

Ослабление ИК-излучения в атмосфере обусловлено полосами поглощения водяных паров, углекислого газа и озона, а также рассеиванием излучения. При проведении разведки и мероприятий по защите объектов необходимо учитывать ослабление собственного или отраженного ИК-излучения в атмосфере за счет рассеяния согласно формуле [5]:

$$P_1 = P_0 e^{-\beta x}, \qquad (2.12)$$

где P_1 – поток излучения, прошедший через слой рассеивающей среды; P_0 – падающий на рассеивающий слой поток излучения; β – коэффициент рассеивания; x – толщина рассеивающего слоя.

Для случая рассеяния излучения объемом газа $\beta = \frac{a}{N\lambda^4}(n-1)^2$, где $a = \frac{16\pi^3 V}{3}$; V – объем газа в м^3; λ – длина волны; n – показатель преломления газа; N – число молекул в единице объема газа.

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

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

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

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

2.5. Демаскирующие признаки радиоэлектронных средств

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

Все демаскирующие признаки, связанные с радиоизлучениями, определяются техническими характеристиками радиосигналов, которые можно разделить на следующие группы: частотные, временные, энергетические, спектральные, пространственно-энергетические, фазовые, поляризационные [5].

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

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

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

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

По спектральным характеристикам радиоизлучений можно судить о распределение энергии между составляющими спектра. Основными спектральными характеристиками являются: ширина спектра, вид спектра

(сплошной, дискретный), относительная величина отдельных спектральных составляющих, форма огибающей спектра.

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

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

Технические признаки радиоизлучений можно разделить на групповые, индивидуальные и оперативные [5].

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

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

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

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

Вопросы для самопроверки

1. Приведите определение технического демаскирующего признака объекта.

2. Перечислите виды демаскирующих признаков.

3. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра.

4. Что относится к демаскирующим признакам объектов в инфракрасном диапазоне электромагнитного спектра?

5. Какие демаскирующие признаки характеризуют радиоэлектронные средства?

6. Частотные демаскирующие признаки радиоэлектронных средств.

7. Какие характеристики радиоэлектронных средств относятся к временным?

8. Какие характеристики радиоэлектронных средств относятся к энергетическим?

9. Что характеризуют пространственно-энергетические характеристики радиоэлектронных средств?

10. О чем можно судить по спектральным характеристикам радиоизлучений?

11. Какие характеристики радиоэлектронных средств относятся к поляризационным?

12. Какие характеристики радиоэлектронных средств относятся к фазовым?

3. СРЕДСТВА ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

3.1. Общие сведения

Принцип действия большинства индикаторов электромагнитного поля основан на широкополосном детектировании электрического поля. Индикаторы обеспечивают возможность обнаружения радиопередающих прослушивающих устройств с любыми видами модуляции.

Представленные на отечественном рынке комплексы для проведения специсследований позволяют в автоматическом режиме решать ряд задач измерений ПЭМИН и облегчают работу инженера-исследователя, повышают производительность его труда.

Некоторые комплексы на основе сканирующих приемников или анализаторов спектра применяются для быстрого анализа спектра ПЭМИН, излучаемых техническим средством, но не обеспечивают высокой точности измерений. При необходимости выдачи предписания на эксплуатацию технического средства, измерения, произведенные при помощи таких комплексов, подлежат обязательной ручной проверке с использованием метрологического измерительного оборудования (измерительных приемников или анализаторов спектра).

Комплексы типа «Навигатор» применимы для проведения достаточно точных измерений ПЭМИН в условиях экранированных помещений (безэховых экранированных камер), но результаты измерений могут быть достоверными только при их тщательной ручной проверке с использованием средств самого комплекса.

1. Автоматизация обнаружения гармонических составляющих тестового сигнала.

Обычно инженер-исследователь ищет гармонические составляющие «на слух», распопознавая искомые компоненты по звуку и форме осциллограммы демодулированного сигнала. Инструментальная реализация такого режима приводит к тому, что автоматическая система, распознающая сигналы по их форме, работает лишь ненамного быстрее квалифицированного инженера-исследователя. Поэтому в первых комплексах данный режим не был реализован, а опознавание производилось по критерию изменения уровней сигналов при включении тестового режима на исследуемом техническом средстве (так называемый «энергетический критерий»). Такой способ дает неплохие результаты: вся работа по обнаружению сводится к двум проходам сканирования диапазона специсследования: при первом проходе запоминается картина шумов при выключенном тестовом режиме, при втором проходе исследуемое техническое средство переводится в тестовый режим, и измеряются уровни всех сигналов, превышающих запом-

ненные шумы на заданное значение порога. Ускорение работы достигается очень существенное: вместо нескольких часов специсследование выполняется за считанные минуты. В результате инженер-исследователь получает таблицу частот и уровней сигналов (типичное количество обнаруженных составляющих – несколько сотен) и может рассчитать зоны разведдоступности. Однако результаты расчета могут оказаться неверными, так как электромагнитная обстановка изменяется со временем. В диапазоне от 9 кГц до 1000 МГц работают тысячи радиостанций и источников радиопомех. Некоторые из них время от времени включаются и выключаются, и если какой-то источник радиоизлучения не работал во время сканирования спектра шумов, а при втором проходе включился, его частота окажется в списке обнаруженных составляющих. Естественно, это может случайным образом изменить рассчитанные размеры зон разведдоступности. Таким образом, оператору приходится вручную проверять все обнаруженные составляющие, на что будет уходить время. По-настоящему эффективно данный способ работает в безэховых экранированных камерах, которые ввиду своей дороговизны доступны очень немногим предприятиям.

В более совершенных комплексах применяется автоматическое опознавание информационных сигналов. Согласно методике инженеру-исследователю предлагается выполнить поиск какой-либо гармонической составляющей вручную или в специальном «полуавтоматическом» режиме, либо создать эталонный образ искомого сигнала при помощи редактора (генератора), либо выбрать ранее созданный образ из библиотеки, после чего комплекс автоматически обнаруживает в эфире сигналы, похожие на заданный сигнал. Для опознавания сигналов в таких комплексах применяется взаимно корреляционная функция. Это более затратный по времени способ, но и существенно более точный.

2. Автоматизация измерения уровней сигналов

Этим свойством обладают практически все современные комплексы.

3. Измерение наводок в сети питания, линиях и коммуникациях

Согласно действующим нормативным документам, измерение наводок в сети питания должно осуществляться при помощи эквивалента сети или пробников напряжения. Эквивалент сети достаточно сложное и относительно дорогостоящее устройство, однако измерения, проведенные с его помощью, обычно точнее измерений, выполненных с помощью пробника напряжения. «Чистая» сеть, имитируемая эквивалентом сети, позволяет измерять создаваемые исследуемым техническим средством наводки в сеть питания, уровень которых на 4–6 дБ выше собственных шумов эквивалента сети, в то время как точность измерений, выполняемых при помощи пробника напряжения, зависит от уровней шума сети питания. Для автоматизированных измерительных систем очень важна возможность использования в своем составе различных приемных устройств: антенн, пробников на-

пряжения, эквивалентов сети. Соответственно, в программном обеспечении комплекса должен быть предусмотрен механизм поддержки дополнительных приемных устройств, а именно, возможность ввода таких параметров, как рабочий диапазон, антенные коэффициенты (коэффициенты затухания или усиления) и их автоматический учет в процессе измерений. Таким механизмом обладают комплексы «Легенда» и «Сигурд».

Особенности функционирования различного рода технических средств радиомониторинга и обнаружения закладных устройств рассмотрим на конкретных примерах их технической реализации.

Существует предположение, что подслушивающие устройства представляют собой исключительно радиопередатчики. Однако злоумышленники используют большое число электронных устройств, которые по принципу действия весьма далеки от радиопередатчиков [25, 26, 27, 28, 30]. Именно в этих случаях нелинейный локатор или локатор нелинейности (ЛН), разработанный в начале 80-х годов, может эффективно обнаруживать и определять местоположение любого электронного устройства, независимо от того находится оно в рабочем состоянии или нет.

К наиболее совершенным программно-аппаратным комплексам для оценки норм эффективности защиты речевой информации можно отнести сходные по своим характеристикам комплексы «Шепот» и «Спрут 7»

Программно-аппаратный комплекс «СПРУТ-7» предназначен для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств в речевом диапазоне частот, образованных за счет акустоэлектрических преобразований.

Комплекс обеспечивает измерение характеристик акустических сигналов, в том числе октавный, третьоктавный анализ и анализ с использованием функции быстрого преобразования Фурье (БПФ), что позволяет с высокой точностью проводить измерения слабых сигналов акустоэлектрических преобразований.

Необходимо указать также на эффективное использование довольно простых и недорогих многофункциональных комплектов для выявления каналов утечки информации таких, например, как «ПКУ-6М» и «Пиранья».

Для выявления технических каналов утечки информации широко применяются досмотровые устройства такие как металлодетекторы, различного рода эндоскопы, рентгенотелевизионные установки.

Область применения металодетекторов (металлоискателей, металлообнаружителей), позволяющих регистрировать запрещенные и опасные металлические предметы в непроводящей среде, постоянно расширяется. В последнее время актуальной стала задача оснащения металлодетекторами

таких сугубо гражданских объектов, как школы, больницы, театры и т.п. Металлодетекторы применяются сегодня также в дефектоскопии (поиск металлических включений в различных материалах), рудной электроразведке, в системах контроля доступа, предотвращения хищений и т.д.

Портативные рентгенотелевизионные установки применяется для проведения мероприятий по обнаружению взрывных устройств в оставленных свертках, сумках, ручной клади, багаже, а также для поиска скрыто установленных средств съема информации в предметах интерьера, мебели, различных бытовых неразборных приборах [46].

Эндоскопы предназначены для осмотра труднодоступных мест в строительных конструкциях, транспортных средствах, контейнерах, узлах технологического оборудования и т.п. с целью выявления взрывных устройств, оружия, контрабанды, а также негласно установленных средств съема информации. Специальное покрытие рабочей части позволяет обследовать содержимое сосудов с агрессивными жидкостями, например, бензобаки. Эндоскопы могут комплектоваться сетевыми осветителями (мощностью 100 ВА) и фототелевизионным трактом, позволяющим получить высококачественное изображение наблюдаемого объекта на экране ЖКИ дисплея.

3.2. Индикаторы электромагнитного поля

Рассмотрим несколько примеров реализации индикаторов поля.

Индикатор поля-частотомер SEL SP-71M «Оберег» (рис.3.1, *а*) является микропроцессорным индикатором поля и предназначен для мгновенного обнаружения любых источников радиоизлучения: радиомикрофонов, в том числе носимых, радиостанций, а также работающих сотовых телефонов стандарта GSM, DAMPS и DECT [56].

а *б*

Рис. 3.1. Индикаторы поля: *а* – частотомер «Оберег», *б* – «DP-20»

Детектор СВЧ-поля DP-20 (рис. 3.1, *б*) представляет собой электронный прибор, предназначенный для световой и звуковой индикации наличия и относительного уровня электромагнитного излучения в диапазоне частот от 900 МГц до 2,5 ГГц [56].

Индикатор позволяет обнаружить электромагнитное поле, оценить уровень сигнала и найти его источник. Возможность выбора режима акустической обратной связи (АОС) или режима звуковой индикации уровня сигнала облегчает поиск радиопередающих устройств.

Для прослушивания акустических сигналов к прибору могут быть подключены головные телефоны, при этом встроенный динамик автоматически отключается.

Десятисегментная логарифмическая светодиодная шкала и прерывистый тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором, тональность звукового сигнала меняется в зависимости от уровня входного сигнала.

Дифференциальный детектор поля «АРК-ДДП» (рис. 3.2) разработан для обнаружения и локализации источников радиоизлучения. Выделяет сигналы микропередатчиков на фоне сильных помеховых полей. Применяется для поиска средств негласного съёма информации, использующих радиоканал в диапазоне частот от 10МГц до 3ГГц. Обнаруживает микропередатчики с любым видом модуляции и произвольной шириной спектра. Имеет малые габариты и автономное питание от встроенного аккумулятора.

Рис. 3.2. Индикатор поля «АРК-ДДП»

Принцип действия прибора основан на широкополосном детектировании входных сигналов. Сигнал, приходящий от источника радиоизлучения, находящегося в ближней зоне, наводит на антеннах прибора напряжения, отличающиеся по амплитуде. Эти два сигнала детектируются, вычитаются друг из друга и усиливаются. Приближение к источнику радиосигнала вызывает щелчки, частота которых пропорциональна расстоянию до источника.

Отличительная особенность прибора заключается в том, что сигналы, приходящие от удалённых радиопередатчиков, наводят на антеннах прибора одинаковые напряжения, поэтому ослабляются во много раз.

3.3. Сканирующие радиоприемники

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

Сканирующие радиоприемники характеризуются следующими основными показателями:

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

Представленные на отечественном рынке модели сканирующих приемников обычно удовлетворяют требованиям по диапазону и скорости сканирования для поиска радиомикрофонов или других источников радиоизлучения, не использующих режим быстрой перестройки рабочей частоты. В то же время возможность обнаружения таких радиомикрофонов или способность контроля технически сложных каналов радиосвязи зависят не только от параметров сканирования радиоприемника, но и от наличия в составе комплекса других средств, обеспечивающих решение подобных задач. В качестве таких средств в настоящее время все чаще используются специализированные комплекты программного обеспечения. В этих условиях особое значение приобретает способность сканирующего радиоприемника эффективно работать в составе автоматизированного комплекса радиоконтроля под управлением персонального компьютера. С этой целью рядом зарубежных и российских компаний производителей были разработаны так называемые «компьютерные» радиоприемники, специально ори-

ентированные на обеспечение эффективного взаимодействия с ЭВМ. Конструктивно такие приемники выполняются либо в виде плат, встраиваемых в ISA-слот компьютера, либо в виде отдельных модулей, подключаемых к компьютеру через порты COM, LPT или PCMCIA. Благодаря такому решению обеспечивается высокая скорость обмена информацией между радиоприемником и компьютером, а отсутствие дополнительных внешних органов управления позволяет достичь небольших значений массогабаритных параметров приемника.

Сканирующий приемник AR5000 (рис. 3.3, *а*) предназначен для контроля радиоэфира в диапазоне частот от 10 кГц до 2,6 ГГц. Приемник обладает высокими эксплуатационными характеристиками и большим набором сервисных функций. Приемник имеет следующие технические характеристики:

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

Сканеры японской фирмы ICOM завоевали широкое признание во сем мире. Новая модель IC-R10 (рис. 3.3, *б*) воплотила в себе все современные технологические достижения, что позволило добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при сохранении небольших габаритов и веса. Ряд функций впервые реализованы в носимом сканере.

а *б*

Рис. 3.3. Сканирующие приемники «AR5000» (*а*) и «ICOM IC-R10» (*б*)

Основные характеристики сканера:

- Широкий диапазон: 0,5-1300 МГц с разрешением 100Гц.
- Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM.
- Спектроскоп. Работает в реальном времени, ширина полосы обзора ±50 или ±100кГц.
- Расширенный набор типов и видов сканирования: каждый из 2-х основных типов сканирования разбит на три вида: сплошное, диапазонное, с

автоматической записью частот, по каналам памяти, по видам модуляции, по банкам памяти.

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

3.4. Анализаторы спектра, радиочастотомеры

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

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

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

Радиотестеры измеряют параметры сигналов, работают со всеми типами модуляции.

Радиочастотомеры предназначены для измерения частоты источника радиосигнала.

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

Примеры технической реализации некоторых перечисленных устройств приведены ниже.

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

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

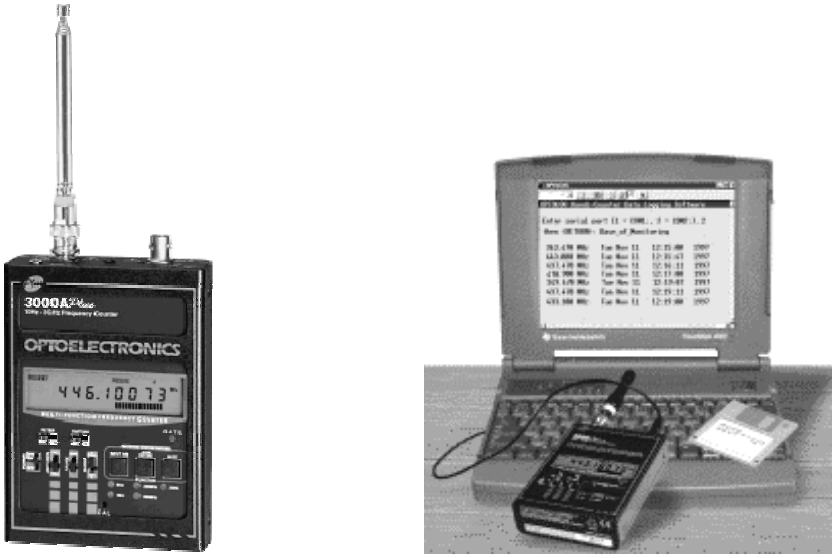
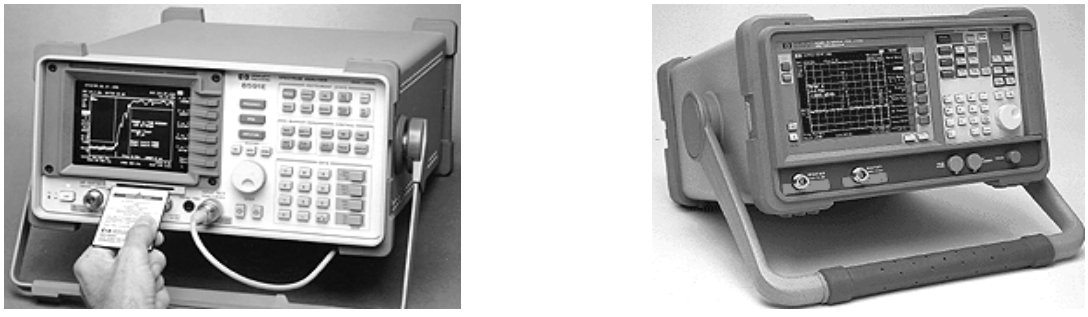


Рис. 3.4. Портативный многофункциональный частотомер «3000A Plus»

Усилители с входным сопротивлением 1 МОм позволяют использовать 3000A Plus для измерения частот и временных характеристик сигналов в электронных схемах [56]. Измеряться могут как периодические, так и импульсные сигналы напряжением до 50 вольт.

Анализатор спектра HP8591E (рис. 3.5, *а*) предназначен для проведения специальных исследований электронно-вычислительной техники и слаботочного оборудования на наличие и уровень побочных электромагнитных излучений и наводок; для контроля радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации об объекте и сравнительного анализа с уже имеющимися, полученными ранее, данными; для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации [56]. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО.



а *б*

Рис. 3.5. Анализаторы спектра «HP8591E HP» (*а*) и «ESA-L1500A» (*б*)

Анализатор спектра HP ESA-L1500A (рис. 3.5, *б*) предназначен для проведения специальных исследований электронно-вычислительной техники и слаботочного оборудования на наличие и уровень побочных элек-

тромагнитных излучений и наводок; для контроля радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации об объекте и сравнительного анализа с уже имеющимися, полученными ранее, данными; для инженерных исследований изымаемых органами МВД технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.); для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации [56]. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО. Диапазон рабочих частот – 9…1,5 ГГц.

3.5. Многофункциональные комплекты для выявления каналов утечки информации

3.5.1. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»

Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М» представляет собой удобную в работе многофункциональную поисковую систему (рис. 3.6).

Рис. 3.6. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»

Система предназначена для выявления [44]:

- средств съема информации с передачей сигнала по существующим проводным коммуникациям;
- утечки речевой информации по акустическому и вибро-акустическому каналам;
- средств съема информации с передачей сигнала по оптическому каналу.

Система содержит комплект датчиков, позволяющих:

- выявить каналы утечки акустической информации через сквозные щели и трещины ограждающих конструкций;
- оценить вибро-акустические свойства ограждающих конструкций и инженерных коммуникаций;
- обнаружить электрические сигналы в слаботочных линиях в полосе частот 0,3…10 кГц;
- обнаружить электрические сигналы в сильноточных линиях в полосе частот 0,03…24, 5 МГц;
- выявить оптическое излучение осветительных приборов, индикаторов, датчиков сигнализации, блоков дистанционного управления в видимом и инфракрасном диапазонах.

В состав комплекта «ПКУ-6М» входят:

- основной блок-анализатор;
- микрофон со звукопроводом;
- вибро-электрический датчик;
- оптический датчик;
- имитатор многофункциональный «ИМФ-2»;
- головные телефоны;
- комплект соединительных кабелей;
- комплект съемных зажимов и щупов;
- сетевой адаптер питания.

Поисковая система «ПКУ-6М» обеспечивает:

- обнаружение сигналов низкой частоты в полосе 0,3…10 кГц;
- прием сигналов с амплитудной (АМ) и частотной (ЧМ) модуляцией в диапазоне частот 30…24500 кГц;
- автоматическую перестройку в рабочем диапазоне частот;
- визуальное отображение спектров принимаемых сигналов на ЖК-дисплее;
- прослушивание принимаемого сигнала при помощи встроенного динамика или головных телефонов;
- запись аудио- сигнала в режимах RF (индикация уровня сигнала в мВ) и AF (индикация уровня выходного сигнала усилителя низкой частоты в дБ) на внутренний носитель.

В режиме SP спектроанализатора сканирование по установленному диапазону частот можно проводить как в ручном, так и в автоматическом режимах. Скорость автоматического режима работы составляет примерно 10 кГц/с с дискретностью 1 кГц.

В режиме панорамы PN на экране дисплея после сканирования одновременно может отображаться полоса частот шириной не более 1440 кГц.

После остановки автоматического сканирования в режиме PN можно выбрать одно из действий:

1. продолжить сканирование в ручном режиме;
2. установить курсор настройки центральной частоты просмотра на выбранный участок панорамы;
3. перейти в режим просмотра спектра в диапазоне ±25 кГц от текущей центральной частоты;
4. возобновить получение панорамы от текущего значения центральной частоты.

Изменение вида модуляции при прослушивании детектированных сигналов производится нажатием соответствующей кнопки.

Осциллографический просмотр низкочастотных сигналов возможен как в режиме AF, так и в режиме RF. В режиме RF осциллограмма AM или FM сигнала приводится после детектора. При переходе в режим AF на экране автоматически появляется осциллограмма низкочастотного входного сигнала анализатора.

Кроме контроля с помощью встроенного громкоговорителя или головных телефонов выявленный аудиосигнал может быть записан на встроенное устройство. Запись осуществляется схемой электронной памяти прибора, состоящей из нескольких банков. Выбор банков памяти при записи осуществляется автоматически.

Устройство позволяет выполнить последовательную запись нескольких сигналов, которые могут быть прослушаны в ходе последующего анализа. Объем памяти позволяет записывать сигналы продолжительностью до 16 мин.

При заполнении памяти прибор продолжает запись аудиосигнала, последовательно стирая предыдущую информацию.

Имеющийся в составе системы многофункциональный имитатор «ИМФ-2» предназначен для имитации работы средств съема информации при проведении поисковых мероприятий и как источник тестирующих сигналов.

Рассмотрим особенности выявления каналов утечки информации.

Акустический канал

При визуальном обследовании помещения отмечаются возможные каналы прямой воздушной проводимости – окна, щели, трещины, вентиляци-

онные каналы. Исследование предполагаемого акустического канала утечки информации проводится по схеме рис. 3.7.

Имитатор в режиме «AUDIO» создает со стороны проверяемого помещения тестовый акустический сигнал с уровнем 70 дБ. Уровень прошедшего через ограждение сигнала измеряется микрофоном и основным блоком, работающим в режиме AF, и характеризует звукопоглощающие свойства ограждающей конструкции.

Если организовать озвучивание помещения речевым сигналом, то через наушники можно оценить его разборчивость.

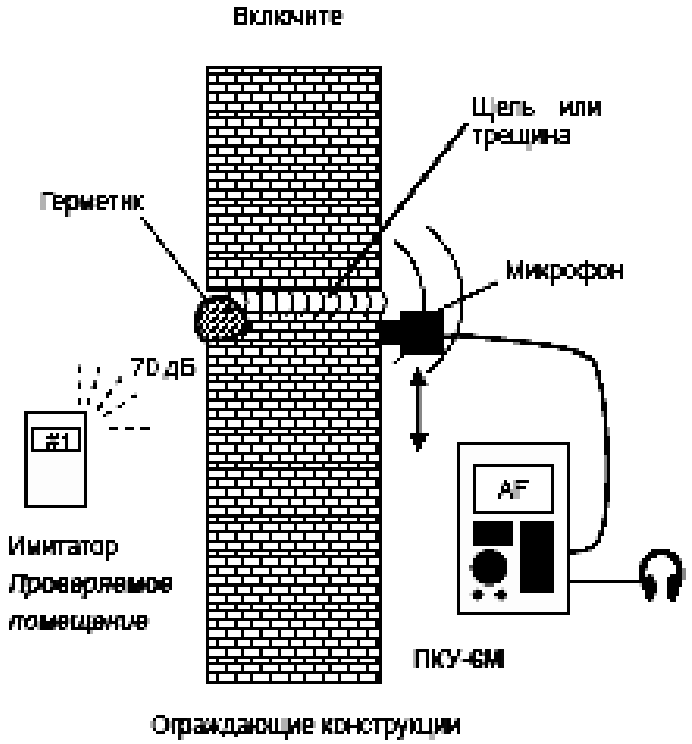


Рис. 3.7. Схема исследования акустического канала

Подобные действия необходимо провести во всех подозрительных местах и выявить места наилучшего прохождения акустического сигнала.

Виброакустический канал

При визуальном обследовании помещения отмечаются все жесткие конструкции (балки, колонны, бетонные стены, трубы и т.п.), выходящие за пределы контролируемой зоны. Исследование предполагаемого виброакустического канала утечки информации проводится по схеме рис. 3.8.

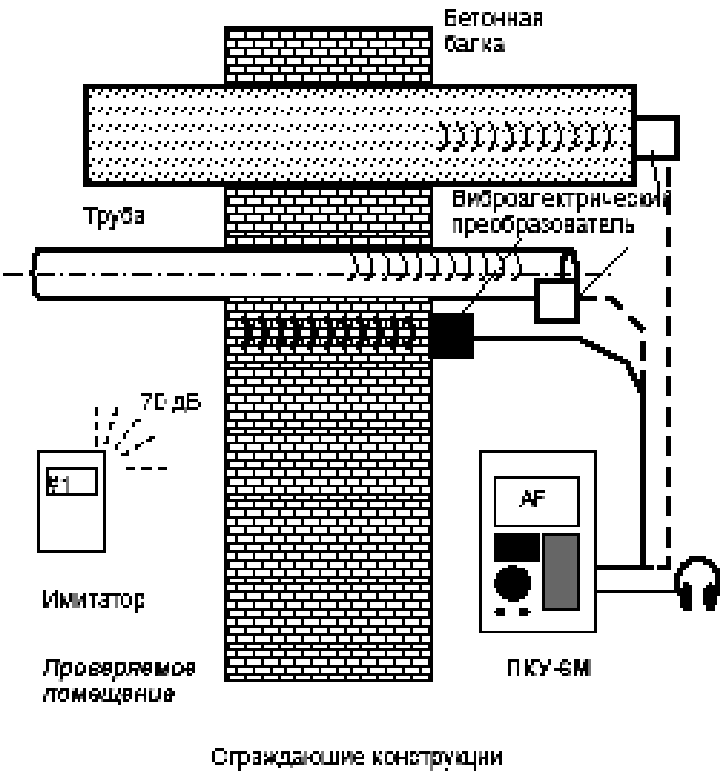


Рис. 3.8. Схема исследования виброакустических каналов

Схема исследования виброакустических каналов такая же как и схема исследования акустических каналов, только микрофон заменяется виброакустическим датчиком, который должен иметь плотный контакт с жесткой конструкцией с усилием порядка 5 кГ.

Имитатор в режиме «AUDIO» создает со стороны проверяемого помещения тестовый акустический сигнал с уровнем 70 дБ. Уровень прошедшего через ограждение сигнала измеряется виброакустическим датчиком и основным блоком, работающим в режиме AF.

Выявление микрофонного эффекта и обнаружение скрытых микрофонов

Перед началом поисковых работ необходимо изучить все проводные коммуникации, выходящие за пределы контролируемой зоны, и провести исследования по схеме рис. 3.9.

Наличие микрофонного эффекта осуществляется следующим образом. Имитатор переводится в режим работы «AUDIO» и последовательно устанавливается на расстоянии 1 м от офисного оборудования. Основной блок подключается через входной комплектный низковольтный кабель к проверяемой проводной линии. Наличие микрофонного эффекта оценивается по появлению сигналов в головных телефонах.

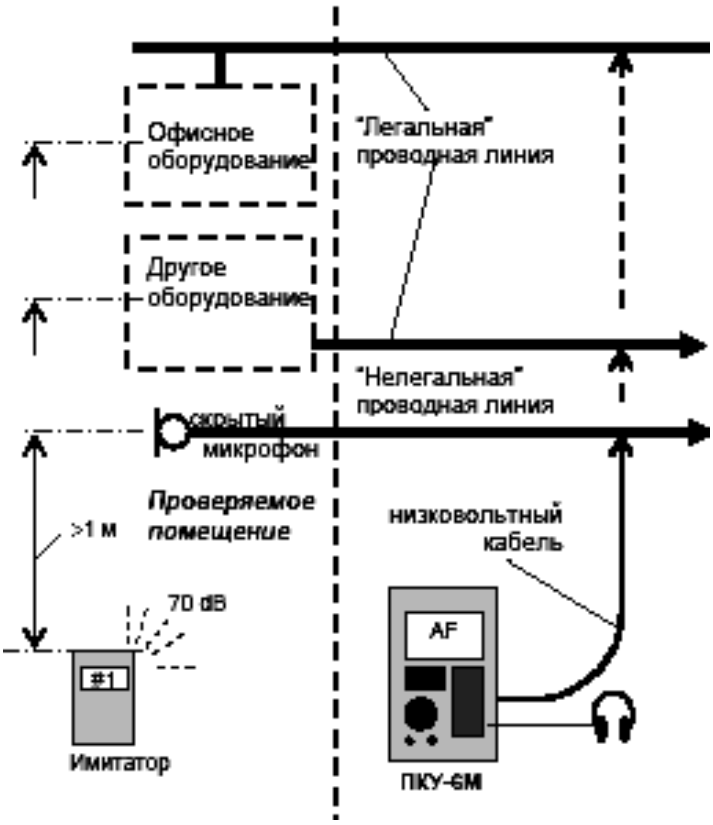


Рис. 3.9. Выявление микрофонного эффекта и обнаружение скрытых микрофонов

Офисное оборудование исследуется при всех режимах его работы.

Для выявления скрытно установленных в ограждающих конструкциях основной блок подключается к проводной линии неизвестного назначения. В линию от основного блока подается постоянное напряжение 15 В с поочередной сменой полярности и включается имитатор. Наличие микрофона оценивается по характерному сигналу в головных телефонах.

Проверка электрических сигналов в сетях электропитания и слаботочных линиях

Этот вид проверки производится по схеме рис. 3.10 и подробных пояснений не требует.

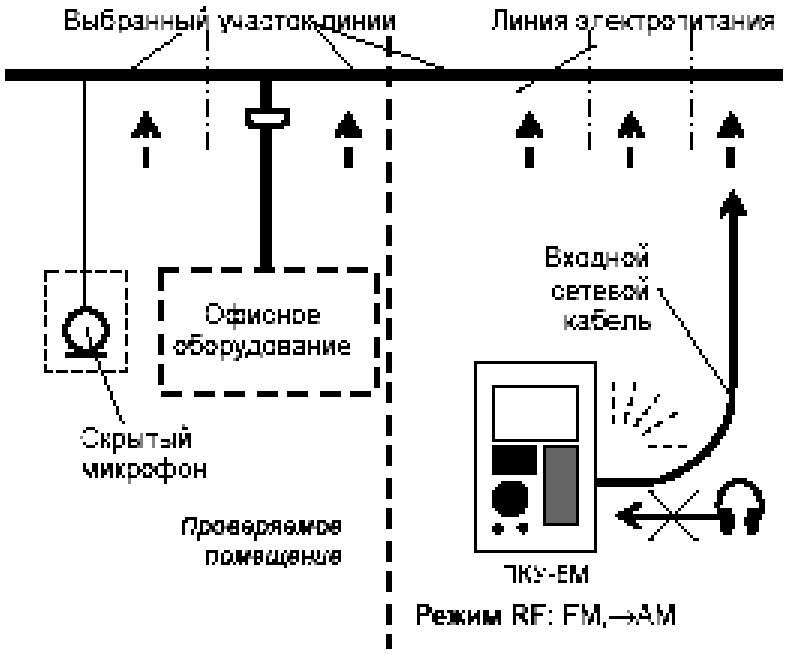


Рис. 3.10. Проверка электрических сигналов в сетях электропитания и линиях

Входной сетевой кабель подключается к проверяемой линии и входному блоку. Поочередно в режимах FM и AM модуляции производится поиск сигналов в линиях.

В режиме анализа спектра производится поиск скрытых микрофонов в линиях. При обнаружении сигнала от скрытно установленного микрофона обследуется проверяемая линия последовательным подключением к различным ее участкам с целью определения максимального уровня принимаемого сигнала. Место нахождения микрофона определяется при включенном встроенном громкоговорителе, используя явление «акустической завязки».

Проверка слаботочных линий

Проверка слаботочных линий осуществляется по схеме рис. 3.10. В этом режиме работы входной сетевой кабель заменяется на низковольтный кабель или кабель с 6-ти или 8-ми контактными адаптерами (рис. 3.11).

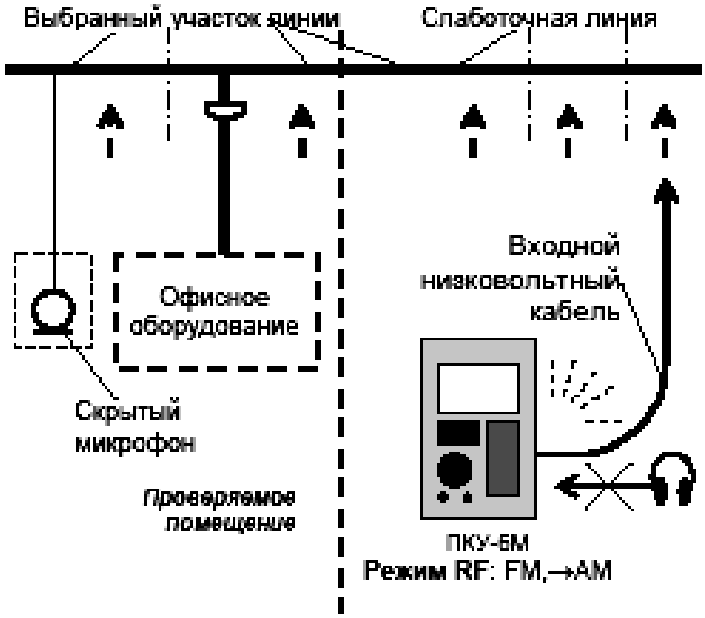


Рис. 3.11. Проверка слаботочных линий

Проверка оптического канала

Проверка оптического канала осуществляется по схеме рис. 3.12.

Перед проверкой определяются источники видимого и инфракрасного излучения, которые могут стать причиной утечки информации по оптическому каналу:

- осветительные приборы;
- датчики охранной сигнализации;
- пульты дистанционного управления;
- световые индикаторы электронной аппаратуры.

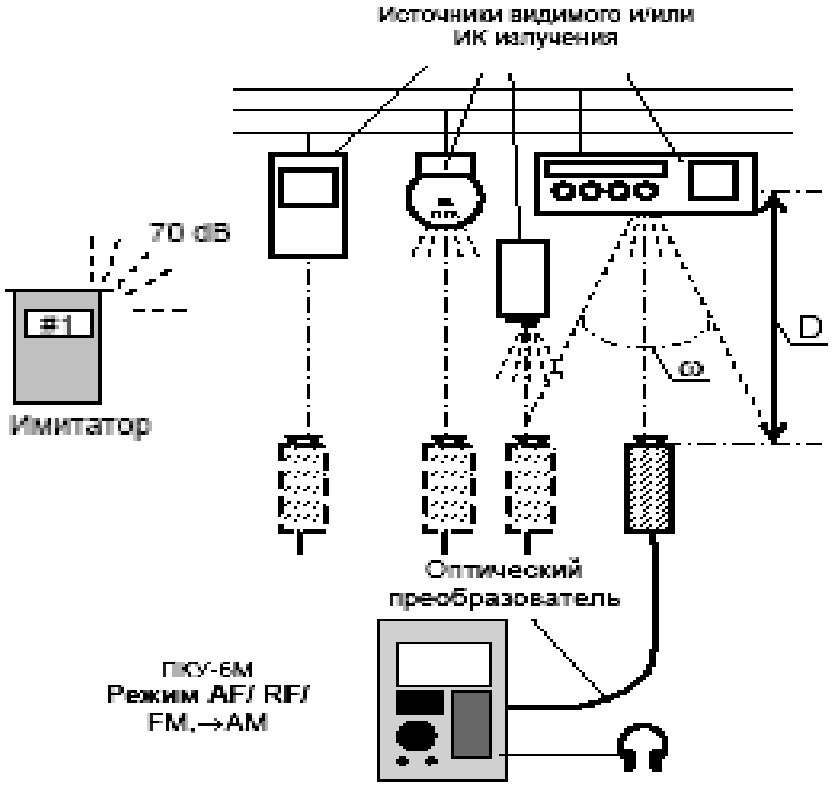


Рис. 3.12. Проверка оптического канала

Имитатор помещается в месте проведения переговоров и совещаний и переводится в режим работы «AUDIO» (озвучивание). На основном блоке устанавливается режим AF и к нему подключаются оптический датчик и головные телефоны. Оптический преобразователь направляется в сторону обследуемых объектов и определяется наличие в головных телефонах характерного тона, соответствующего сигналу имитатора.Удаляя оптический преобразователь от проверяемого оборудования, определяется направление и расстояние, на котором прием сигналов еще имеет место. Указанные операции повторяются в режиме RF.

3.5.2. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»

Близким по назначению к «ПКУ-6М» является комплект ST 031 «Пиранья» [45]. Он предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получе-

ния информации, а также для выявления и контроля естественных и искусственно созданных каналов утечки информации (рис. 3.13).

Прибор состоит из основного блока управления и индикации, комплекта преобразователей и позволяет работать в следующих режимах:

- высокочастотный детектор-частомер;
- сканирущий анализатор проводных линий;
- детектор ИК-излучений;
- детектор низкочастотных магнитных полей;
- дифференциальный низкочастотный усилитель;
- виброакустический приемник;
- акустический приемник.

Рис. 3.13. Комплект ST 031 «Пиранья»

Переход прибора в любой из режимов осуществляется автоматически при подключении соответствующего преобразователя. Информация отображается на графическом ЖКИ дисплее с подсветкой, акустический контроль осуществляется через специальные головные телефоны, либо через встроенный громкоговоритель. Управление прибором производится с помощью 16-ти кнопочной клавиатуры. Обеспечивает возможность запоминания в энергозависимой памяти 99-ти изображений.

Прибор позволяет обрабатывать поступающие низкочастотные сигналы в режиме «осциллограф» либо «спектроанализатор» с индикацией численных параметров. В ST 031 «Пиранья» предусмотрен вывод на дисплей контекстной помощи в зависимости от режима работы. Возможен выбор как русского, так и английского языка.

ST 031 «Пиранья» выполнен в носимом варианте. Для его переноски и хранения используется специальная сумка, приспособленная для компактной и удобной укладки всех элементов комплекта. Предварительный этап подготовительных мероприятий предстоящей контрольно-поисковой работы состоит в заблаговременном детальном изучении объекта. При этом изучаются условия расположения объекта, а также его конструктивные особенности. Кроме того, важное значение на этом этапе имеют оформление интерьера помещения (состав и размещение мебели) и оснащенность техническими средствами (ПЭВМ, ксероксы, факсы, телефонные аппараты, бытовая техника и т. п.). Считается целесообразным полученные данные в

произвольной форме протоколировать. На этом этапе следует также выявить наличие и расположение проводных и других потенциально опасных коммуникаций.

1. Использование прибора для выявления каналов утечки информации в радиочастотном диапазоне

Эти каналы могут быть созданы как преднамеренно за счет использования заинтересованными органами и организациями специальных технических средств съема информации, так и возникнуть естественным образом за счет побочных электромагнитных излучений технических средств обработки информации. В любом случае возникает необходимость классификации сигналов в радиочастотном диапазоне по совокупности критериев.

1.1. Один из практических подходов к классификации радиосигналов

С точки зрения решения задач контроля защиты информации с использованием прибора «Пиранья», все радиосигналы, попадающие в его рабочий диапазон, можно достаточно обоснованно разделить на «опасные» и «неопасные».

«Опасные» радиосигналы могут быть созданы как внутренними, так и внешними источниками. На практике встречается довольно большое число их самых разнообразных сочетаний.

Обычно к числу чисто «внутренних опасных» радиосигналов относят:

- сигналы «радиозакладок» (радиомикрофоны, телефонные радиотрансляторы и т.п.).
- сигналы радиомаяков;
- сигналы несанкционированно включенных в помещении радиостанций и радиотелефонов;
- побочные электромагнитные излучения ПЭВМ и других технических средств обработки информации.

К категории «опасных» в сочетании «внутренние-внешние» принято относить радиосигналы, источниками которых могут быть:

- радиомикрофоны с выносным акустическим микрофоном;
- телефонные радиоретрансляторы, установленные на линии связи за пределами помещения (но вблизи него);
- радиостетоскопы, установленные с наружной стороны ограждающих помещение поверхностей;
- вынесенные передатчики скрытых видеокамер;
- устройства внешнего высокочастотного облучения.

1.2. Методы поиска и локализации источников опасных радиосигналов

В случае обнаружения потенциально опасного радиосигнала следует двигаться в направлении возрастания его уровня. Контроль за уровнем принимаемого сигнала необходимо осуществлять по показаниям индикаторов уровня на экране дисплея прибора и по частоте щелчков звуковой сигнализации в режиме «TONE».

Метод акустической завязки основан на возникновении положительной акустической обратной связи между микрофоном «радиозакладки» и динамиком прибора «Пиранья». При этом обязательно включение звуковой сигнализации прибора в режиме «AUD» для вывода на динамик демодулированного сигнала. Эффект акустической завязки возникает только в отношении радиозакладки, в которой применены обычные виды модуляции – амплитудная и частотная (узкополосная или широкополосная).

Признаком возникновения акустозавязки является появление характерного «писка», тон и интенсивность которого изменяются при приближении динамика прибора к микрофону радиозакладки.

Эффективность выбора того или другого метода во многом зависит от особенностей, присущих потенциально опасным радиосигналам и их источникам.

1.3. Особенности потенциально опасных радиосигналов и их источников

Радиомикрофоны [45]. Широкое распространение имеют радиомикрофоны с параметрической стабилизацией частоты передатчика. Основная их особенность – большие пределы девиации несущей частоты (до нескольких мегагерц). Поэтому для локализации радиомикрофонов такого типа наиболее целесообразно использование метода «акустозавязки».

В качестве высокопрофессиональных средств негласного добывания информации применяются радиомикрофоны с вынесенным передатчиком. Их основная особенность – разнос мест установки микрофона и собственно радиопередатчика (вплоть до выноса в другое помещение). В этом случае необходимо сочетание метода «акустозавязки» и амплитудного метода. При этом для локализации микрофона необходимо использовать метод «акустозавязки», а радиопередатчика (в проверяемом помещении или за его пределами) – амплитудный метод.

Высокопрофессиональными средствами являются и радиомикрофоны с закрытым или маскированным радиоканалом. Их основная особенность состоит в том, что принятый и демодулированный сигнал не несет в себе информации об акустическом фоне помещения. Это определяется использованием для закрытия (маскирования) радиоканала методов инверсии спектра, цифровых методов передачи и сложных видов модуляции. Поэтому в основе их обнаружения и локализации должен лежать амплитудный метод с дополнением его анализом осциллограмм и спектрограмм.

Другие источники потенциально опасных радиоизлучений [45]. К ним относятся радиостетоскопы, скрытые видеокамеры с радиоканалом передачи информации, радиозакладки в ПЭВМ, радиомаяки, средства пространственного высокочастотного облучения, несанкционированно включенные средства связи (радиостанции, радиотелефоны, телефоны с радиоудлинителями).

Для создания акустического фона и для активизации радиозакладок с акустопуском следует подготовить и разместить в контролируемом помещении тестовый источник звука.

Если не имеется ограничений на скрытность проведения работ, то наилучший эффект дает сочетание амплитудного метода и метода акустозавязки. При проведении скрытного поиска необходимо применять амплитудный метод с прослушиванием детектированных сигналов через головные телефоны.

Особое внимание при работе следует обратить на радиоизлучения в диапазоне 60–640МГц, наиболее типичном для использования радиомикрофонами и телефонными радиоретрансляторами. Поиск осуществляется путем последовательного обхода помещения (объекта) с движением вдоль стен и обследованием мебели и других предметов. При отсутствии ограничений на использование метода акустозавязки динамик встроенного громкоговорителя прибора следует ориентировать в сторону обследуемых поверхностей и предметов.

При приближении антенны прибора «Пиранья» к месту размещения радиозакладки напряженность электромагнитного поля возрастает и повышается уровень сигнала на его входе.

При достаточном приближении к источнику радиочастотомер осуществляет захват частоты и показывает в строке экрана ее значение по результатам нескольких измерений. Путем уменьшения громкости, изменения границ динамического диапазона, увеличения вручную порога срабатывания детектора, постоянного наблюдения за показаниями частотомера сужается зона обследования и, тем самым, локализуется место установки радиозакладки с погрешностью в пределах 10–15 см.

В случае применения в качестве радиозакладки телефонов стандарта DECT или GSM, помимо индикации повышения уровня сигнала в нижней строке, на индикаторе появится надпись DECT или GSM.

Аналогично поиску радиомикрофонов осуществляется поиск телефонных радиоретрансляторов. При этом для их активизации необходимо снять трубки всех телефонных аппаратов. Поиск проводится в два этапа. Сначала проверяются на наличие закладных устройств сами телефонные аппараты. Установленный в аппарате радиоретранслятор проявляется точно так же как и радиомикрофон. Далее поиск телефонных радиоретрансляторов осуществляется путем обхода помещения вдоль абонентской телефонной линии и выявления на ней мест с максимальным уровнем радиосигнала. При обходе антенну прибора необходимо ориентировать в разных плоскостях на минимально возможном расстоянии от линии. Практически всегда существует необходимость проверки линии вплоть до основного распределительного щита.

Поиск радиостетоскопов имеет определённые особенности, обусловленные способами их применения (установка вне контролируемого помещения). Поэтому для обнаружения сигналов радиостетоскопов необходимо обследовать все доступные внешние поверхности ограждающих конструкций.

Поскольку средой распространения виброакустических колебаний могут являться трубы отопления и водоснабжения, то проверке подлежат и эти коммуникации.

Принципиально передатчики видеокамер могут работать на частотах до 2300 МГц. Обнаружение сигнала (похожего на сигнал яркости) на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры. Локализация таких средств осуществляется амплитудным методом.

Применительно к пространственному высокочастотному облучению основной является задача выявления факта создания этого искусственного канала добывания информации. Обычно она решается в два этапа [45]. На первом этапе выявляется факт облучения помещения высокочастотным сигналом. На втором этапе отслеживается отклик на зондирующий высокочастотный сигнал. При этом необходимо ориентироваться на следующие факторы. Остронаправленный луч электромагнитной энергии может быть сформирован только на очень высоких частотах (800–900 МГц и выше). Радиоволны этого диапазона распространяются в условиях прямой видимости между источником излучения и облучаемыми предметами, поэтому в качестве основных путей их проникновения в контролируемое помещение определяют прежде всего оконные проемы. Переизлучающими объектами могут быть обычные для данного помещения технические средства, обладающие так называемым микрофонным эффектом. К ним обычно относят динамики бытовых громкоговорителей, акустические системы даже выключенной аудиоаппаратуры, телефонные аппараты с электрическим звонком и т.п. Переизлученный на частотах высших (чаще всего второй или третьей) гармоник сигнал локализуется в непосредственной близости от облучаемых предметов и имеет модуляцию акустическим фоном помещения.

Исходя из этого, может быть определен следующий порядок работы. Для выявления факта высокочастотного облучения поочередно провести обследование потенциально опасных оконных проемов. По графическому индикатору оценить стабильность частоты излучения. Перейти в любое из соседних помещений (ориентированных окнами в ту же сторону) и повторить проверку в районе каждого из его оконных проемов.

Высокочастотное облучение вполне вероятно, если:

- частота принимаемого сигнала лежит (или очень близка) в пределах указанного диапазона;
- стабильность частоты высокая;
- модуляция сигнала отсутствует.

2. Использование прибора для выявления каналов утечки информации по проводным линиям различного назначения

Рассмотрим приёмы выявления искусственно созданных каналов утечки информации по проводным линиям на основе использования специальных технических средств [45]. Основными видами проводных линий, для анализа которых предназначен прибор «Пиранья», являются линии электросети (высокопотенциальные линии), а также абонентские телефонные линии и линии систем пожарной и охранной сигнализации (низкопотенциальные линии).

В целом приёмы и методы, применяемые для проверки проводных линий названных видов, одинаковы. Подключение к ним осуществляется с использованием универсального адаптера. Анализу методом сканирования подвергается общий диапазон от 0 до 15МГц. Вывод результатов сканирования производится в виде изображения панорамы с однотипным представлением измеренных параметров. Функции органов управления прибором одинаковы (вне зависимости от вида проверяемой линии).

3. Использование прибора для выявления каналов утечки информации в инфракрасном диапазоне

Принципиально следует рассматривать два вида таких каналов утечки информации [45]. Один из них создается за счет применения специальных технических средств с передачей перехваченной информации в инфракрасном диапазоне. Другой канал основан на облучении стекол оконных проемов направленным лучом источника инфракрасных излучений и приеме отраженного сигнала, промодулированного речевым сигналом.

Для выявления обоих каналов утечки необходимо провести одинаковые подготовительные мероприятия. Прежде всего следует правильно выбрать время проведения проверки, а именно такое, когда в окна контролируемого помещения не попадают прямые солнечные лучи. В самом помещении необходимо выключить лампы накаливания и источники интенсивного теплового излучения. Специфика инфракрасных закладок предполагает необходимость обеспечения прямой видимости между передатчиком закладки и приемником инфракрасных излучений. Поэтому в помещении путь прохождения излучения передатчика наружу может проходить только через оконные проемы. С учетом этих особенностей, поиск опасных сигналов следует начинать от окон помещения, передвигаясь вглубь его. Признаком наличия инфракрасного излучения является появление окрашенных сегментов шкалы индикатора уровня и щелчков звуковой индикации в режиме «TONE». Анализ обнаруженных сигналов может производиться на слух в режиме «AUD», а также визуально с использованием встроенных осциллографа и анализатора спектра. Локализация источников инфракрасного излучения наиболее точно осуществляется сочетанием амплитудного метода и метода акустозавязки. При этом порядок действий та-

кой же как и при работе в режиме высокочастотного детектора-частотомера.

4. Использование прибора для выявления каналов утечки информации по низкочастотным магнитным полям

Для таких каналов характерно то, что они возникают при использовании по целевому назначению санкционированных средств (ПЭВМ, переговорных устройств, систем звукоусиления, магнитофонов, телефонов и т.д.). Поэтому одной из основных задач следует считать исследование таких средств на наличие, интенсивность и дальность низкочастотного магнитного поля. Сопутствующими могут считаться задачи поиска скрытой (несанкционированно проложенной) проводки и обнаружения работающих диктофонов.

Перед проведением работ целесообразно выключить в помещении люминесцентные светильники, а антенну прибора, при необходимости, включить в дифференциальном режиме (переключатель на корпусе антенны поставить в положение «к белой точке»).

Потенциальные источники опасных низкочастотных магнитных полей следует проверять раздельно, включая их в работу поочередно.

При исследовании технических средств необходимо оценить дальность распространения магнитных полей и особенности их спектра. Для этого первоначально необходимо разместить магнитную антенну в непосредственной близости от исследуемого объекта и зафиксировать по осциллограмме относительный уровень поля. Удаляясь от исследуемого средства и изменяя пространственную ориентацию антенны, оценить дальность уверенного приема низкочастотного сигнала.

Применительно к усилителям звуковой частоты, имеющим выходной трансформатор, следует оценить дальность уверенного (разборчивого) приёма речевого (тестового) сигнала.

Такая оценка может послужить основой для правильного выбора мест установки соответствующих средств по отношению к наружной стороне помещения и варианта их совместного расположения в помещении. При необходимости включить режим «SA», проанализировать спектрограмму и записать ее в энергонезависимую память.

Для поиска скрытой проводки необходимо последовательно обойти все стены помещения, располагая магнитную антенну в непосредственной близости к ним. Зафиксировать область возрастания уровня поля и путем перемещения антенны по горизонтали и вертикали определить прохождение трассы скрытой проводки.

5. Использование прибора для оценки эффективности виброакустической защиты и звукоизоляции помещений

Оценка эффективности виброакустической защиты помещения обычно проводится в два этапа. На первом этапе защита, если она имеется, должна

быть выключена и произведена проверка собственно виброакустических свойств ограждающих помещение поверхностей. Для этого необходимо виброакустический датчик прикреплять в различных местах проверяемых поверхностей (стен, дверей, окон, по возможности пола и потолка) с внешней, по отношению к контролируемому помещению, стороны. Включить источник тестового звукового сигнала. Он может размещаться либо в обычном месте ведения конфиденциальных разговоров, либо на определённом расстоянии *L* от обследуемой поверхности.

Уровень звука обычно устанавливают соответствующим громкой речи (74 дБ). Для калиброванных источников звука расстояние «*L*» выбирают в пределах 1,0…2,0 м. Сначала на качественном уровне (путём прямого прослушивания) оцениваются виброакустические свойства обследуемых поверхностей, а затем, переходом в режим «SA», количественно оцениваются амплитуды частотных составляющих тестового сигнала.

На втором этапе, если это предусмотрено, оценивается эффективность системы виброакустической защиты. Для этого на каждой поверхности как качественно на слух, так и количественно по спектрограмме определяется соотношения уровней тестового и маскирующего сигнала, а также выявляются «не прикрытые» составляющие спектра. Это служит объективной основой коррекции амплитудно-частотной характеристики источников маскирующего сигнала.

Согласно общепринятым правилам разборчивость речевых сигналов гарантированно не восстанавливается, если маскирующий шум (помеха) в 4–5 раз (16 дБ) превышает их уровень. Полное исключение признаков речи достигается при 8-ми кратном превышении уровня сигнала помехой, создаваемой системой активной защиты.

Оценку звукоизоляции помещений также целесообразно проводить в два этапа. На первом этапе, используя тестовый источник сигнала с уровнем звука, соответствующим громкой речи, установить соответствие между этим уровнем и показаниями прибора в режимах осциллографа и анализатора спектра. Для этого необходимо разместить акустический излучатель источника звука и микрофон прибора на некотором фиксированном расстоянии. Обычно его выбирают в пределах 1,0…2,0 м.

На втором этапе оцениваются звукоизоляционные свойства ограждающих конструкций, эффективность системы активной защиты (зашумления), а также возможность утечки речевой акустической информации через элементы вентиляции, различного рода ниши, сквозные отверстия и т.п.

Для оценки звукоизоляционных свойств ограждающих конструкций тестовый источник звука может быть расположен либо в обычном месте ведения конфиденциальных разговоров, либо на расстоянии от обследуемой поверхности.

Размещением микрофона в различных местах смежных (выше и ниже расположенных) помещений качественно на слух и количественно по спектрограмме определяется дальность перехвата речевого сигнала из данного помещения и оценка снижения уровня звукового сигнала за счёт свойств ограждающих поверхностей, а также наличие наименее ослабленных составляющих спектра. Последнее даёт возможность принять обоснованное решение о необходимости дополнительной защиты, в том числе и активной, и выбор характеристик средств защиты.

Поскольку воздуховоды систем вентиляции являются наиболее опасными каналами утечки речевой акустической информации, то они подлежат обязательной проверке. Для этого микрофон прибора необходимо ввести в выходное (входное) отверстие воздуховода каждого из смежных помещений. Качественно на слух оценивается прохождение и разборчивость сигнала от тестового источника, а по показаниям прибора в режиме осциллографа или анализатора спектра – его ослабление при прохождении по воздуховоду до места размещения микрофона. Правильная оценка ослабления может быть получена только в том случае, если имеется детальная схема системы вентиляции.

3.6. Многофункциональный комплекс радиомониторинга и выявления каналов утечки информации «АРК-Д1ТИ»

Комплекс (рис. 3.14) позволяет проведение специальных исследований технических средств на сверхнормативные побочные электромагнитные излучения и наводки (ПЭМИН), радиомониторинг, поиск технических каналов утечки информации, технический анализ, специальные функции [56].

АРК-Д1ТИ – сертифицированный (в системе Гостехкомиссии РФ) многофункциональный портативный комплекс третьего поколения для выявления технических каналов утечки информации и радиомониторинга.

Используемый способ обнаружения радиомикрофонов и устройство его осуществления защищены патентом РФ.

Комплекс решает задачи:

- оценка защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации;
- оценка защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства, системы и их коммуникации;
- оценка защищенности речевой конфиденциальной информации от утечки за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах;

• контроль в реальном масштабе времени радиоэлектронной обстановки в районе защищаемых объектов военного и государственного назначения в пределах контролируемой зоны, выявление различного рода нарушений, связанных с несанкционированным включением излучающих средств, находящихся на территории защищаемых объектов, и контроль эффективности работы средств защиты.

Рис. 3.14. Комплекс «АРК-Д1ТИ»

В состав комплекса входят:

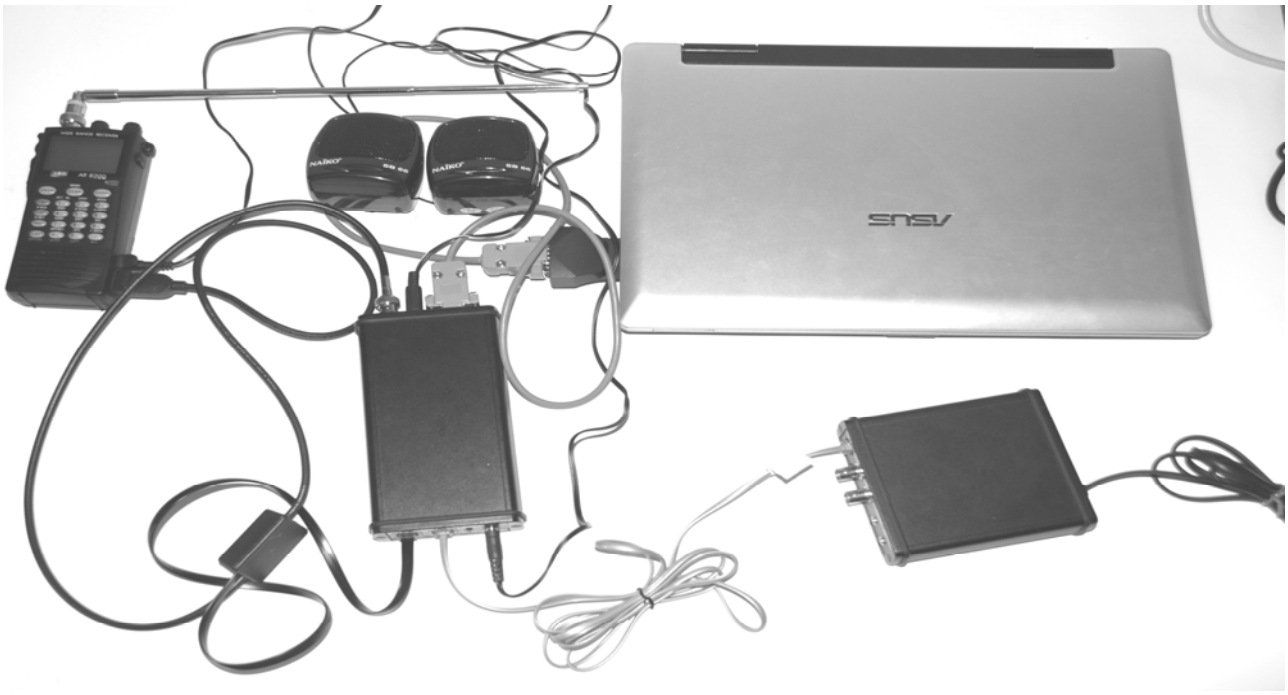
- центральный модуль АРК-Д1ТИ в кейсе;
- широкополосная измерительная антенна АРК-А7И;
- широкополосная антенна АРК-А2М (комплект из трех антенн);
- широкополосная наружная антенна АРК-А5;
- пакет программ СМО-ДХИ;
- IBM совместимая ПЭВМ.

3.7. Комплекс RS turbo

Комплекс RS turbo (рис. 3.15) выполняет все функции комплекса RS turbo Mobile-L, однако позволяет сканировать радиодиапазон вплоть до 12 ГГц с дополнительным конвертером [62]. С помощью конвертера RS/L комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне от 0,6 кГц до 10 МГц, а также в инфракрасной части оптического диапазона.

В частности, для анализа проводных и оптических каналов используется конвертер RS/L, а для нейтрализации выявленных источников радиоизлучений – программируемый генератор RS/N (до 1800 МГц). С помощью антенного коммутатора RS/K комплекс может контролировать радиообстановку с помощью нескольких антенн, предназначенных для различных диапазонов или установленных в пространственно разнесенных помещениях. Контроллеры акустических систем RS/Z используются для обнаруже-

ния и определения местоположения радиомикрофонов методом акустического зондирования в удаленных помещениях.



а

б

Рис. 3.15. Комплекс RS turbo: *а* – общий вид, *б* – схема включения

Общая схема соединений аппаратуры комплекса RS turbo: компьютера, сканирующего радиоприемника, местной акустической системы и контроллера показана на рис. 3.15, *б*. На лицевой стороне корпуса контроллера RS turbo находятся светодиод, индицирующий наличие напряжения питания, которое поступает от собственного блока питания, телефонный разъём для подключения к последовательному порту управления приемником, телефонный разъём шины I2C для подключения дополнительных периферийных устройств, а также гнездо для подключения акустических колонок «Speaker». На задней стороне контроллера находятся разъём для подключения последовательного интерфейса RS232 компьютера (COM-порт), гнездо круглого разъема питания 12 вольт и разъём CP-50 для подключения выхода промежуточной частоты приемника AR8200.

К контроллеру поставляется комплект специальных соединительных кабелей, различных для каждого типа приемников.

Сканирование

Сканирование – это базовая операция, которая предшествует обнаружению, классификации и идентификации источников излучений (сигналов). В процессе сканирования выявляются занятые участки исследуемого частотного диапазона и оцениваются спектры присутствующих в нем сигналов. Частота настройки сканирующего приемника изменяется дискретно с фиксированным шагом 8 МГц и на каждом шаге вычисляемый контроллером RS turbo результат измерений уровней принимаемых во всем спектре сигналов заносится в компьютер. В анализаторе RS turbo быстрое сканирование выполняется с широким (200 кГц) или узким (12,5 кГц) шагом. По результатам сканирования компьютер формирует спектральную панораму исследуемого диапазона, в которой каждому значению частоты настройки соответствует измеренный спектр сигнала. Операции сканирования выполняются в порядке их размещения в списке операций задания. Это дает возможность в первую очередь просматривать те участки спектра, где вероятность найти излучения несанкционированных источников выше. Один частотный диапазон можно включать в задание несколько раз, чтобы реализовать различные алгоритмы идентификации и классификации излучений.

Выполнив один цикл сканирования, программа составляет таблицу, в которой каждому значению частоты настройки ставится в соответствие измеренный последовательным анализатором контроллера RS turbo спектр сигналов в полосе анализа 8 МГц, снятый для сигналов, превышающих заданный порог, с разрешением 12,5 кГц. Эта таблица называется спектральной панорамой. Программа комплекса RS turbo позволяет формировать спектральные панорамы с учетом данных, полученных в ходе текущего и любого числа предшествующих циклов сканирования. После выполнения первого цикла сканирования таблица спектральной панорамы сохраняется

в памяти компьютера. На следующем цикле формируется новая (текущая) таблица, а значения уровней в таблице предыдущей панорамы модифицируются в соответствии с выбранным методом обработки:

−обновление (в таблицу записывается новое значение, а старое стирается);

−накопление (в таблицу записывается больший из двух уровней);

−усреднение (в таблицу записывается среднее двух уровней).

Первый из перечисленных методов обычно используется в процессе обнаружения излучений, а следующие два – для сбора данных, характеризующих обстановку в заданных диапазонах при продолжительных наблюдениях со статистической обработкой результатов измерений. Накопление максимальных значений обеспечивает наиболее полный учет всех излучений, появлявшихся за время наблюдения. Накопление средних значений позволяет при большом числе циклов сканирования свести к нулю уровни случайных сигналов, например, импульсных помех. Текущая панорама отображается на экране зеленым цветом и показывает уровни, измеренные в текущем цикле сканирования.

Данные, полученные в результате обработки уровней предшествующих циклов сканирования, отображаются красным цветом и располагаются на заднем плане. В любой момент после остановки сканирования таблица панорамы, отражающая результаты выполненных циклов сканирования, может быть сохранена в виде файла (файл панорамы спектра, расширение .pan) с заданным программой или пользователем именем. Спектральные панорамы, характеризующие обстановку в заданном диапазоне частот, называются диаграммами загрузки диапазона. Такие панорамы на экране отображаются синим цветом и используются в качестве фона для обнаружения «неизвестных» излучений.

При необходимости данные, отражающие результаты предшествующих циклов сканирования, могут быть удалены из списка командой очистки. При этом в исходную таблицу панорамы записываются нулевые уровни. Если программа работает с несколькими заданиями, то таблица уровней составляется и модифицируется для каждого из них. При этом на экране отображаются панорамы спектров активного задания. В процессе анализа проводных линий с помощью конвертора RS/L plus текущий спектр зеленого цвета выводится на экран на фоне спектра красного цвета, полученного на предыдущем цикле.

Для повышения скорости работы комплекс RS turbo выполняет сканирование с помощью последовательного анализатора спектра с разрешением 12,5 КГц с шагом 8 МГц. После запуска сканирование ведется с указанным шагом по сетке частот. Начальная и конечная частоты указанного в задании диапазона заменяются ближайшими частотами этой сетки. На каждом шаге контроллер RS turbo измеряет уровни принимаемых сигналов, т.е.

снимает спектр на широкополосном выходе промежуточной частоты приемника, и передает данные в компьютер.

Обнаружение

Обнаружение – базовая операция выявления всех радиоизлучений (сигналов), уровень которых в заданном диапазоне превосходит установленное в задании пороговое значение (порог обнаружения). В процессе обнаружения программа оценивает параметры сигнала: ширину спектра, максимальный уровень, несущую частоту, а также классифицирует обнаруженные излучения, распределяя их по группам в соответствии с определенными признаками. Обнаруженные излучения автоматически классифицируются программой RS turbo по следующим признакам:

−«известные» и «неизвестные»;

−«обнаруженные ранее» и «вновь появившиеся»;

−«стандартные» и «нестандартные».

Анализ

Операции анализа необходимы для выявления среди множества обнаруженных сигналов «опасных» излучений, которые могут быть созданы передатчиками подслушивающих устройств. Идентификация (опознавание) сигналов подслушивающих устройств в программе RS turbo выполняется автоматически или в ручном режиме с помощью следующих операций:

−анализ гармонического состава излучений;

−корреляционный анализ откликов на акустические импульсы;

−спектральный анализ;

−временной и спектральный анализ сигналов на выходе демодулятора.

Кроме того, в процессе анализа откликов на импульсы акустического зондирования программа измеряет расстояния от колонок акустической системы комплекса до микрофона и определяет местоположение микрофона в помещении (локализация источника излучения).

3.8. Комплексы измерения ПЭМИН

Программно-аппаратный комплекс «СИГУРД» (рис. 3.16) представляет собой одну из самых совершенных систем оценки защищенности технических средств по каналу ПЭМИН и предназначен для проведения специальных исследований различных технических средств по выявлению, распознаванию и измерению сигналов их побочных электромагнитных излучений с максимальной степенью автоматизации процедур [48].

Система создана на базе анализатора спектра фирмы IFR (MARCONI) или других производителей, стандартного IBM-совместимого персонального компьютера (настольного или Notebook) и комплекта антенн. Могут быть применены любые антенны, предназначенные для работы в диапазоне от 9 кГц до 2 ГГц. Рекомендуется применение активных широкополосных

антенн. Антенный коэффициент вводится в управляющую программу и учитывается автоматически при выборе соответствующей антенны. Замена антенн в процессе измерений осуществляется оператором в соответствии с сообщениями управляющей программы.

Основным отличием данной системы от аналогичных разработок является четырёхэтапное обнаружение и измерение сигналов и полностью автоматическое, адаптивное распознавание частот (сигналов) ПЭМИН и автоматическое дистанционное управление параметрами тест-режимов на исследуемой ПЭВМ (на базе типового IrDA канала).

Рис. 3.16. Программно-аппаратный комплекс «СИГУРД»

На первом этапе выполнения задания в автоматическом режиме осуществляется фильтрация всех входных сигналов по энергетическому критерию (превышение на заданную величину над уровнем шумов). Далее система выполняет коррекцию каждого выявленного сигнала, уточняя его частоту. На третьем этапе осуществляется корреляционный двухступенчатый анализ сигналов в сравнении их с эталоном, хранящимися в файловой библиотеке. Эталон сигнала синтезируется оператором по спектрограмме реального сигнала в процессе формирования задания. Предусмотрено выделение сигналов, корреляционные характеристики которых не позволяют программе сделать однозначный вывод, и выдача их на экран оператору для принятия решения. На последнем этапе выполняется измерение выявленных «опасных» сигналов.

Все спектры, зафиксированные в процессе специальных исследований, могут быть сохранены для последующего анализа. Данная функция позво-

ляет дополнительно вести анализ спектров методом «наложения», при котором сравниваются два спектра, снятых в разных режимах работы исследуемого устройства. Изменения спектра по сравнению с сохранённым при наложении выделяются цветом.

Управляющая программа позволяет управлять всеми необходимыми режимами работы анализатора спектра. Все задаваемые оператором параметры запоминаются в виде «задания». Библиотека заданий сохраняется для последующего использования, в том числе любое задание может быть использовано в последующем без изменений или с любыми изменениями. Выполнение любого задания может быть приостановлено оператором в любой момент и продолжено или запущено сначала или продолжено с изменёнными в случае необходимости параметрами.

Предусмотрен и ручной режим работы с анализатором спектра при управлении всеми его функциями от компьютера. Анализатором спектра можно управлять и автономно с помощью его органов управления. При этом при возврате под управление компьютера оператор может продолжить выполнение задания с параметрами, предусмотренными заданием или с введёнными с пульта управления анализатора спектра вручную.

Задача расчёта требуемых параметров исследуемых устройств решается отдельным программным модулем, использующим результаты измерений ПЭМИН исследуемого устройства в виде файла данных и дополнительные данные, вводимые оператором. Итогом расчёта является таблица данных измерений и расчётов, предназначенная для включения в отчёт.

Анализатор спектра может работать непрерывно от автономного источника электропитания до полутора часов, что позволяет в ряде случаев минимизировать уровень помех при измерениях. Рекомендуемые измерительные антенны также предусматривают автономное электропитание. Таким образом, при использовании компьютера «Notebook», весь комплекс может быть мобильным и автономным.

Программно-аппаратный комплекс «ЛЕГЕНДА» (рис. 3.17) предназначен для автоматизированного контроля побочных электромагнитных излучений и наводок, а также выявления и контроля акустоэлектрических преобразований в исследуемых технических средствах [57].

Комплекс «Легенда» создан на базе современных приборов ведущих производителей радиоизмерительной аппаратуры: «Agilent Technologies», «Rohde Schwarz», «Tektronix», «Advantest» и др.

Комплекс работает под управлением специального программного обеспечения, разработанного на основании действующих нормативно-методических документов Гостехкомиссии России.

В состав комплекса входят:

- радиоизмерительный прибор (обычно анализатор спектра фирмы «Agilente Technologies» E4411B, 9 кГц – 1,5 ГГц) с опциями;

- антенный коммутатор;
- система измерительная «Альбатрос» (9 кГц – 1 ГГц);
- эквивалент сети EMCO 3810/2;
- управляющая ЭВМ (обычно NoteBook) с интерфейсом GP-IB (National Instruments) и GP-IB кабелями;
- комплект для обнаружения акустоэлектрических преобразований;
- специальное программное обеспечение: управляющая программа, расчетные программы, комплект тестов для ПЭВМ (под WIN 95/98).

Рис. 3.17. Программно-аппаратный комплекс «ЛЕГЕНДА»

Отличительные особенности комплекса:

- два этапа обнаружения ПЭМИН исследуемых технических средств в автоматизированном режиме (устранение «чужих сигналов»):
- выделение пика на фоне шумов («энергетический» критерий);
- распознавание образа сигнала (сравнение эталонного сигнала с сигналом приемного устройства в текущий момент);
- достоверность и повторяемость результатов измерений;
- возможность применения различных антенных систем в том числе и старого парка аппаратуры (RFT);
- возможность полуавтоматического обнаружения и измерения сигналов, измерения по сформированным шаблонам (наибольшая скорость проведения исследований);
- автоматическое формирование протоколов измерений;

• использование самых распространенных текстовых редакторов – «Microsoft Office», «Word Pad» и «Note Pad» при оформлении отчетных документов.

Для обнаружения и измерения уровней сигналов создается образ эталонного сигнала с помощью специального редактора эталонов. Определяется программа проведения исследований.

По команде оператора комплекс сканирует указанный в настройках диапазон, обнаруживает и измеряет сигналы ПЭМИН ПЭВМ.

Имеется возможность прерывать работу для подключения или изменения характеристик антенн. Измеренные значения заносятся в таблицу, которая затем может сохраняться в виде файла на диске.

Переносной комплекс для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения «НАВИГАТОР-П6-Г» (Е4407В) представлен на рис. 3.18. Он предназначен для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности [57].

Рис. 3.18. Переносной комплекс «НАВИГАТОР-П6-Г»

Применяемое специальное программное обеспечение (СПО) позволяет максимально автоматизировать процессы измерений, обработки их результатов, выполнения необходимых расчетов и подготовки отчетной документации по результатам выполненных исследований.

В программно-аппаратном комплексе реализованы четыре метода поиска ПЭМИН:

- метод сравнения панорам;
- аудио-визуальный метод;

- экспертный метод;
- параметрически-корреляционный метод.

Первые три метода позволяют осуществлять поиск ПЭМИН в автоматизированном режиме. Четвертый метод обеспечивает полностью автоматический поиск и выявление информативных ПЭМИН.

В состав комплекса входят измерительная и управляющая подсистемы. Связь между подсистемами осуществляется с помощью интерфейсов RS-232 или GPIB. С помощью измерительной подсистемы комплекса проводятся измерения электрической и магнитной составляющих электромагнитного поля, а также наводок в проводных коммуникациях. Параметры измеренных сигналов передаются из измерительной подсистемы в управляющую, где происходит их обработка, представление на экране в удобном для оператора виде и хранение в виде файлов.

Программно-аппаратный комплекс позволяет:

- в автоматическом и автоматизированном режимах обнаруживать ПЭМИ тестируемой аппаратуры и формировать список обнаруженных ПЭМИ с регистрацией частоты, уровня ПЭМИ, полосы пропускания и антенны, при которых производилось обнаружение;
- в автоматизированном режиме верифицировать список обнаруженных ПЭМИ при включенном и выключенном тесте на исследуемой аппаратуре;
- Отображать на мониторе компьютера спектры обнаруженных сигналов;
- проводить ручную верификацию списка обнаруженных ПЭМИ, используя осциллографический режим работы анализатора для наблюдения демодулированного тестового сигнала с одновременным прослушиванием теста в звуковом диапазоне частот на встроенных динамиках;
- проводить обработку полученных результатов и расчет зон разведдоступности ПЭМИ и коэффициента защищенности объекта в соответствии с утвержденными методиками;
- проводить инженерные исследования специальных технических средств (радиостанций, радиомикрофонов, систем съема информации и т.д.).

3.9. Нелинейные локаторы

Модель радиолокационного наблюдения в условиях нелинейной локации

Отечественный нелинейный локатор появился в 1993 г. и был представлен моделью «Циклон». В настоящее время на рынке услуг по техническим средствам защиты информации представлено большое число разнообразных типов локаторов, отличающихся друг от друга в основном по четырем параметрам: тип излучения (непрерывный или импульсный); час-

тота излучения; мощность излучения; регистрация количества гармоник – одна (вторая), две (вторая, третья).

На основе имеющихся экспериментальных и физических представлений процесс нелинейной локации в общих чертах полностью аналогичен традиционной локации для случая наблюдения объектов с активным ответом в режиме опознавания.

Существенным отличием нелинейной локации от классического наблюдения (обнаружения) объектов с активным ответом является прямое преобразование падающей на объект энергии зондирующего сигнала в энергию высших гармоник. В связи с этим модель радиолокационного наблюдения (обнаружения) в условиях нелинейной локации можно классифицировать как наблюдение с полуактивным ответом, что связано с отсутствием потребления энергии объектом от специального источника питания.

Нелинейным объектом называется объект, обладающий нелинейной вольт-амперной характеристикой (ВАХ). К ним относятся диоды, транзисторы, микросхемы, контакты металл-окисел-металл (МОМ-диод). К простейшему нестабильному МОМ-диоду относится и классическая двуокись железа – ржавчина.

$$i_{\text{вых}}(t) = i_0 + \alpha e_s(t) + \beta e_s^2(t) + \gamma e_s^3(t) + \ldots \qquad (3.1)$$

где $e_s(t)$ – входной сигнал на нелинейном элементе. Из (2.1) следует, нелинейность ВАХ обуславливает появление в выходном сигнале за счет детектирования постоянной составляющей e_0, основной гармоники с амплитудой, умноженной на коэффициент α и высших гармоник основной частоты, амплитуды которых пропорциональны соответствующим коэффициентам.

Пусть входной сигнал представляет собой гармоническое колебание вида:

$$e_s(t) = A_0 \cos\omega t, \qquad (3.2)$$

где A_0 – амплитуда сигнала, $\omega = 2\pi f$ – круговая частота сигнала в радианах/сек, f – частота сигнала, Гц.

Подставляя (3.2) в (3.1) и проводя тригонометрические преобразования над степенными функциями $\cos\omega t$, получим отклик нелинейного элемента в виде:

$$i_{\text{вых}}(t) \approx i_0 + \beta A_0^2 + (\alpha A_0 + 1{,}25\gamma A_0^3)\cos\omega t + 0{,}5\beta A_0^2 \cos 2\omega t + 0{,}25\gamma A_0^3 \cos 3\omega t \ldots \qquad (3.3)$$

Принцип образования высших гармоник в полупроводниковых приборах, содержащих p-n-переходы, можно пояснить с помощью эквивалентной схемы замещения «зондирующая антенна – полупроводниковый диод». Модель нелинейного объекта в виде вибраторной антенны, подключенной на вход смесителя на полупроводниковом диоде, изображена на рис. 3.19.

Мощность на гармониках, излучаемая объектом и, следовательно, эффективность обнаружения растет при увеличении мощности излучения ло-

катора $P_{изл.}$, снижении частоты его излучения f и номера принимаемой гармоники N. Кроме того, чем ниже частота излучения локатора, тем меньшие значения имеют коэффициенты затухания, что также ведет к увеличению мощности сигнала от объекта.

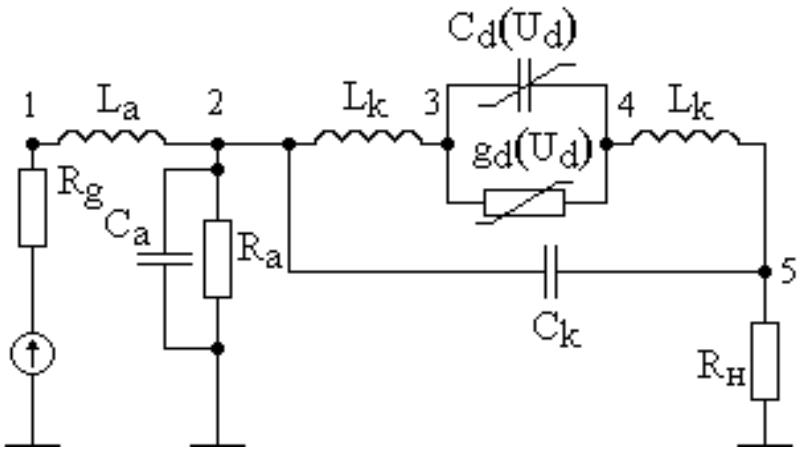


Рис. 3.19. Электрическая схема замещения ЛН

Технология нелинейной локации

Рассмотрим один из способов повышения достоверности обнаружения полупроводниковых устройств с помощью ЛН [34].

Антенна ЛН облучает объект для определения наличия в нем электронных компонентов. Когда высокочастотный сигнал облучает полупроводниковые соединения, он возвращается на гармонических частотах с определенными уровнями, благодаря нелинейным характеристикам соединения. Но ложные срабатывания также могут возникнуть из-за того, что места соединения двух различных металлов или коррозионные металлические конструкции также вызывают гармонический отраженный сигнал вследствие своих нелинейных характеристик. Такие соединения называются ложными.

На рис. 3.20 показаны вольт-амперные характеристики полупроводникового и ложного соединений. Из-за различного характера нелинейных характеристик полупроводникового и ложного соединений составляющие 2-й и 3-й гармоник в отраженном сигнале будут иметь различное соотношение. Когда ЛН облучает полупроводник, вторая гармоника отклика превосходит третью по интенсивности. При облучении ложного соединения имеет место обратная картина: отклик на 3-й гармонике имеет более высокий уровень, чем на 2-й.

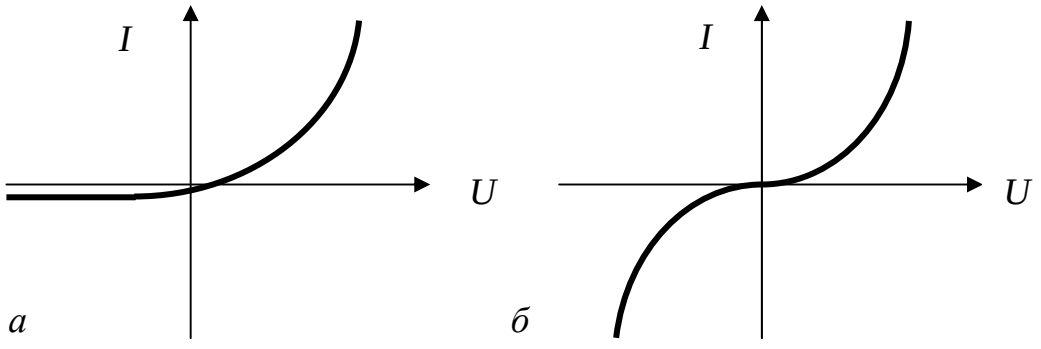


Рис. 3.20. Вольт-амперные характеристики полупроводникового и ложного соединений

Для ЛН, имеющего возможность анализа 2-й и 3-й гармоник, очень важно, чтобы приемные тракты гармоник были частотно изолированы друг от друга и не оказывали взаимного влияния. Сравнение большого числа НЛ различного производства свидетельствует, что большинство из них не имеет хорошей частотной изоляции в приемных трактах. В результате этого чистый полупроводник может иметь более сильный отклик на третьей гармонике, в то время как ложное соединение – на второй. Следовательно, даже если прибор имеет возможность приема отклика на обеих гармониках, то достаточно сложно отличить настоящий полупроводник от ложного соединения.

Эффект затухания

Большинство моделей ЛН использует непрерывное излучение в форме узкополосного сигнала. В последнее время все большее применение находят ЛН с импульсным режимом работы, имеющем ряд преимуществ. Преимущества заключаются в меньшем потребление средней мощности от аккумуляторных батарей при большой скважности периодических зондирующих импульсов и в простоте демодулятора амплитудно-модулированного сигнала. Это объясняется следующими факторами. В импульсном режиме приемник принимает сигналы с частотой, приемлемой для восприятия человеческого слуха и зрения, при выключенном на этих интервалах времени передатчике. что обеспечивает снижение габаритов и энергоемкости источников питания. С другой стороны, для использования эффекта затухания ЛН непрерывного излучения обязательно должен иметь в приемном тракте высококачественные усилители с небольшим уровнем шума и хороший демодулятор для обеспечения качественного выделения аудио сигнала. При импульсном излучении с частотой следования импульсов выше порога частотного диапазона слышимости для качественной демодуляции аудио сигнала достаточно иметь простейший демодулятор амплитудно-модулированного сигнала.

Промышленные образцы ЛН

Измеритель вторичных полей (детектор нелинейных переходов) «NR 900 EM» (рис. 3.21) предназначен для поиска электронных устройств, содержащих полупроводниковые компоненты, независимо от их функционального состояния [57].

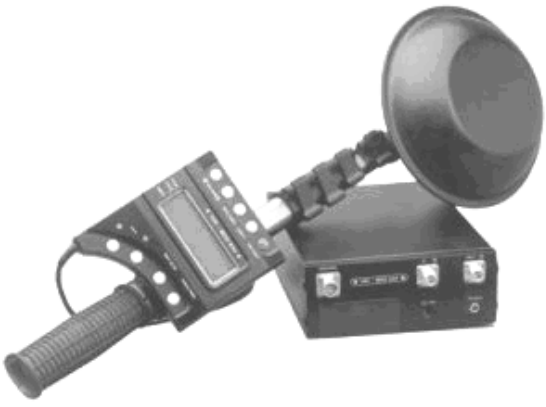


Рис. 3.21. Нелинейный локатор «NR 900 EM»

Устройство обеспечивает возможность поиска радиомикрофонов, в том числе с дистанционным управлением, микрофонных усилителей проводных микрофонов, средств негласного контроля информации инфракрасного и ультразвукового диапазонов, средств звуко– и видеозаписи.

Энергетический потенциал локатора обеспечивает эффективный поиск электронных устройств в ограждающих строительных конструкциях (пол, потолок, стены), в предметах интерьера и мебели.

Остронаправленная антенная система, широкий диапазон регулировок основных параметров изделия обеспечивают высокую точность локализации местоположения искомых устройств и облегчают проведение поисковых мероприятий.

Одновременный прием второй и третьей гармоник зондирующего сигнала, визуальная индикация их уровней, а также режим выделения огибающей отраженного сигнала (режим «20К»), позволяют оператору отличить сигналы, отраженные от полупроводниковых радиоэлементов, от сигналов естественных (коррозийных) нелинейных отражателей.

Устройство обеспечивает возможность работы в условиях помех от сигналов сотовой связи стандарта GSM-1800.

Применение совместно с изделием «NR 900 EM» комплекта зондовых антенн с согласующим устройством позволяет обследовать труднодоступные полости, в том числе экранированные.

Дальность обнаружения штатного имитатора – не менее 0,7 м в режиме излучения максимальной мощности и максимальной чувствительности. В качестве имитатора используется полупроводниковый диод 2Д521А, размещенный в защитном кожухе.

Индикация обнаружения – визуальная на четырехстрочном ЖКИ и звуковая – на головные телефоны.

Устройство представляет собой портативный прибор, состоящий из антенной системы, передатчика и двух приемников, настроенных на удвоенную и утроенную частоты сигнала передатчика. Управление режимами работы осуществляется с помощью выносного пульта управления и индикации. Моногармонический зондирующий сигнал передатчика преобразуется на нелинейных (полупроводниковых) элементах искомого радиоэлектронного устройства в полигармонический. Вторая и третья гармоники этого сигнала переизлучаются, регистрируются приемниками и уровни принятых гармоник представляются оператору в визуальной и звуковой форме.

Локатор состоит из трех конструктивно независимых блоков: приемопередатчика, антенной системы, пульта управления и индикации, соединяемых между собой кабелями. Антенная система и пульт управления и индикации в рабочем положении закреплены на раздвижной телескопической штанге.

Органы индикации расположены на экране ЖКИ пульта управления и индикации. На рис. 3.22. показан вид отображаемой на ЖКИ информации.

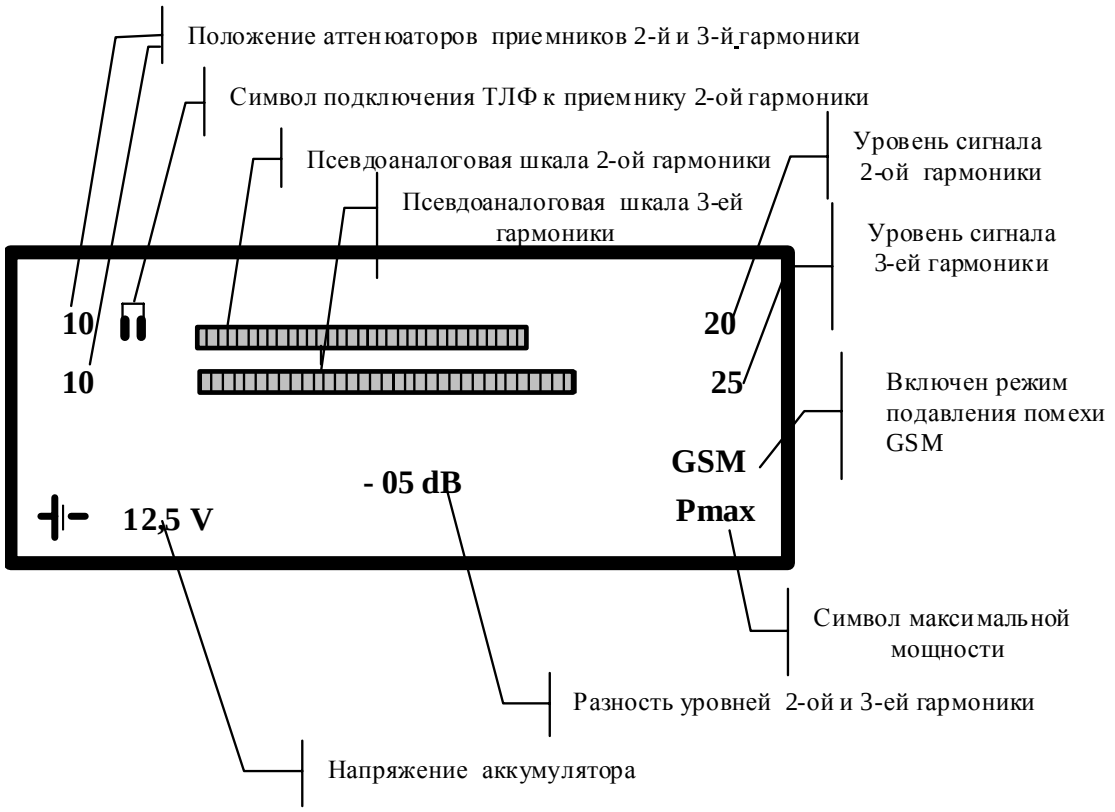


Рис. 3.22. Пульт управления

В первой и второй строках индицируется уровень ослабления аттенюаторов приемников, относительный уровень сигналов второй и третьей гармоник в псевдоаналоговом и цифровом виде и в одной из этих строк – значок ⊓, который указывает, к какому приемнику изделия подключены головные телефоны.

В середине третьей строки индицируется разность уровней второй и третьей гармоник.

Нелинейные локаторы «Октава» (рис. 3.23) рекомендуются для применения при проведении поисковых и досмотровых мероприятий, с целью обнаружения несанкционированной установки и проноса в помещение технических средств съема и передачи информации, для обнаружения предметов, не имеющих в своем составе полупроводниковых элементов, но снабженных специальными маркерами, с целью защиты от хищений.

Нелинейные локаторы «Октава» являются сложными радиотехническими устройствами, состоящими из антенной системы (приемные и передающая антенны), передатчика и одного или двух приемников, настроенных на удвоенную (Октава-В, Октава-К, Октава-М) и утроенную частоту сигнала передатчика (Октава-3М) [57].

Имеется регулировка выходной мощности и усиления приемников.

Рис. 3.23. Нелинейные локаторы «Октава-3М» и «Октава-К»

Нелинейные локаторы «Октава-3М» также имеют режим – «20К», позволяющий выделять огибающую гармоник зондирующего сигнала, и, что особенно важно, возможность приема одновременно по двум каналам 2-ой и 3-ей гармоник. Это позволяет с большей достоверностью отличать сигналы от устройств, подлежащих обнаружению, от сигналов, излучаемых естественными нелинейными образованиями (например, корродированные поверхности).

3.10. Комплекс для измерениия характеристик акустических сигналов СПРУТ-7

Комплекс СПРУТ-7 (рис. 3.24) обеспечивает проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления помещений, измерение уровней электрического и магнитного полей и наводок на проводные коммуникации, проведение статистической обработки результатов измерений [63].

Комплекс может использоваться при измерении и гигиенической оценке шумов и вибрации в жилых и производственных помещениях на соответствие санитарным нормам.

Специальное программное обеспечение комплекса СПРУТ-7 не требует от пользователя каких-либо особых навыков работы на ПЭВМ, кроме знания общих правил работы в среде WINDOWS.

Основные элементы комплекса имеют автономное питание, что делает его мобильным и удобным в эксплуатации.

Подключение модуля сопряжения к ПЭВМ и его питание осуществляется по шине USB.

Технические характеристики и возможности комплекса представлены в приложении.

В программно-аппаратный комплекс «Спрут-7» входят:

1. Измерительная подсистема на базе анализатора шума и вибраций 1-го класса точности SVAN в составе:

- измерительный модуль с октавным анализом, третьоктавным анализом и функцией БПФ;

- измерительный микрофон;
- измерительный акселерометр;
- измерительные щупы;
- измерительная пассивная антенна EMCO-6511 с рабочим диапазоном частот 0,2–5000 кГц либо аналогичная;
- адаптер – усилитель для подключения измерительных щупов и антенн; стойка для установки измерительного модуля;
- зарядное устройство.

Рис. 3.24. ПАК «Спрут-7»

2. Подсистема источника тестового акустического сигнала в составе:
- модуль источника тестового акустического сигнала;
- экранированная акустическая система, используемая при проведении измерений акустоэлектрических преобразований;
- стойка для установки акустической системы;
- зарядное устройство.

3. Подсистема управления:
- модуль сопряжения с ПК;

• ПЭВМ типа «ноутбук»;

• специальное программное обеспечение.

4. Комплект оборудования для обеспечения автономного электропитания объектов ВТСС.

Специальное программное обеспечение позволяет работать с комплексом как с измерительным прибором, а также проводить измерения и обрабатывать результаты в соответствии с методикой ФСТЭК.

3.11. Металлодетекторы

Общие сведения. Одновременно с расширением области применения металлодетекторов происходит процесс уточнения предъявляемых к ним требованиям. В настоящее время наиболее востребованными на рынке являются металлодетекторы, обеспечивающие [32]:

• способность обнаруживать металлы любого типа (ферромагнитные и неферромагнитные) с чувствительностью, достаточной для регистрации малых количеств металла;

• высокую селективность, помехозащищенность и пропускную способность;

• соответствие требованиям заказчика по типу конструкции, дизайну и условиям эксплуатации.

Разновидностями магнитных методов являются индукционные токовихревые с различными видами намагничивающего поля и магнитоэлектрические с использованием естественного геомагнитного поля земли или искусственного магнитного поля.

Наибольшее применение в устройствах, применяемых для выявления оружия и взрывных устройств на людях, посещающих охраняемые объекты, сегодня нашли токовихревые методы [32]. Металлодетектор должен обеспечивать селективное обнаружение определенных металлических или металлосодержащих объектов поиска (ОП) на фоне металлических предметов личного пользования (ПЛП), обычно имеющихся у посетителей. Селективное обнаружение – способность устанавливать факт наличия ОП на фоне одновременного присутствия ПЛП и не давать ложных тревог от ПЛП при отсутствии объектов поиска. Селективное обнаружение может осуществляться только при наличии у ОП характерных признаков. Под этими признаками понимаются какие-либо постоянные их свойства, выявляемые в том или ином реализуемом в металлодетекторе физическом методе, по которому имеются наибольшие различия между ОП и основной частью множества ПЛП.

Рассмотрим подробнее метод вихревых токов при гармоническом намагничивании [32]. Он основан на наличии у ОП основных признаков, присущих металлам: электропроводности и магнитной проницаемости.

Вихревые токи – это токи, протекающие в проводящей среде по замкнутому пути и индуцированные в ней изменяющимся магнитным полем.

Возбуждение вихревых токов осуществляется переменным магнитным полем, создаваемым специальной катушкой, по которой протекает переменный электрический ток. Электромагнитная энергия, проникающая в металлический предмет, частично превращается в тепло, а частично переизлучается.

В зависимости от вида формируемого намагничивающего поля различают метод гармонического поля и метод импульсного поля (метод переходных процессов).

При использовании гармонического метода ОП намагничивается суммой гармонических полей не более трех (чаще всего двух) частот. При использовании метода переходных процессов намагничивание производят импульсами сложной формы, которые можно теоретически представить рядом Фурье (бесконечной суммой гармоник с определенными амплитудами и начальными фазами). Металлический предмет, помещенный в магнитное поле гармонической формы, сам становится источником переменного магнитного поля, изменяющегося с той же частотой. Характерными признаками ОП являются особенности их амплитудно-частотных (АЧХ) и фазочастотных (ФЧХ) характеристик. Это значит, что электрофизические свойства материалов объекта поиска, а также геометрические размеры его элементов приводят к тому, что при некотором значении частоты намагничивающего поля амплитуда и фазовый сдвиг сигнала, переизлучаемого ОП, будут при конкретной ориентации иметь отличия от множества ПЛП.

Фазовый сдвиг поля, переизлучаемого металлическим предметом, больше у массивного предмета, к которому ближе ОП, чем у тонкостенного, что более характерно для ПЛП. Это связано с воздействием на намагничивающее поле реакции вихревых токов, протекающих ближе к поверхности металла. С глубиной из-за поверхностных вихревых токов уменьшается напряженность электромагнитного поля. Эти токи оказывают экранирующее влияние на проникновение поля, что одновременно вызывает их ослабление и нарастающий с глубиной сдвиг по фазе по отношению к намагничивающему полю. Глубина проникновения δ электромагнитных полей и вихревых токов в металл зависит от частоты:

$$\delta \cong \frac{1}{\sqrt{2\pi f g \mu}},$$

где: f – частота, g – электропроводность, μ – магнитная проницаемость.

Из формулы видно, что глубина проникновения вихревых токов в металл уменьшается с ростом частоты. Поэтому на высоких частотах массивный металлический предмет и тонкостенный (одинаковой площади и формы, изготовленные из одного и того же материала), окажутся источниками одинаковых переизлученных полей. Поэтому на высоких частотах нельзя отличить массивный предмет от немассивного.

Теория вихревых токов дает возможность при различных частотах намагничивающего поля определить изменение активной и реактивной составляющих комплексного сопротивления катушки в зависимости от электропроводности, размера и формы предмета, помещенного в катушку.

Теория базируется на уравнении Максвелла. Из решения этого уравнения вытекает ряд формул, показывающих зависимости комплексного сопротивления катушки от электропроводности, магнитной проницаемости материала и размеров предмета, помещенного в нее. Эти зависимости показывают также, что имеется максимум реактивной составляющей комплексного сопротивления катушки, соответствующий определенным параметрам (размерам, материалу), находящегося в ней предмета.

Рассмотрим влияние на характеристики магнитного момента, индуцированного в проводящем предмете, вида материала, из которого он изготовлен.

Пусть круглый, тонкий плоский неферромагнитный диск с радиусом r, толщиной l, обладающий электропроводностью g намагничивается однородным синусоидальным во времени электромагнитным полем. Поле направлено перпендикулярно к плоскости диска и имеет параметры: амплитуда напряженности магнитного поля Hm, круговая частота ω. Тогда при некоторых частотах ($\omega < 0{,}5\omega_{рез}$) намагничивающего поля вихревой ток обуславливает появление в диске индуцированного магнитного момента P с амплитудой:

$$Pm = 0{,}42 \cdot 10^{-6} \gamma \lambda \omega r^4 Hm,$$

отстающего по фазе приблизительно на 90° от намагничивающего поля.

При некоторых частотах (больших резонансной частоты $\omega_{рез}$) вихревой ток отстает по фазе на 180° от намагничивающего поля, а следовательно, создаваемый им магнитный поток через плоскость диска направлен навстречу потоку индукции намагничивающего поля и почти компенсирует его. В этом случае магнитный момент отстает на 180° от намагничивающего поля, а его амплитуда определяется выражением $Pm = 6\, r^3\, Hm$.

Приведенные зависимости для амплитуды магнитного момента сохраняются для квадрата со стороной $a = 2r$. Для тонкой плоской прямоугольной пластины толщиной d с размерами сторон a, an, где n – произвольное целое число, амплитуда магнитного момента будет в n раз больше. В целом эти зависимости сохраняются и для предметов более сложной формы.

Индуцированный магнитный момент неферромагнитного проводящего предмета в основном определяется третьей и четвертой степенями его меньшего размера в плоскости, перпендикулярной намагничивающему полю, и в меньшей степени зависит от других его геометрических характеристик.

Особенности намагничивания ферромагнитного проводящего предмета заключаются в следующем. С изменением частоты намагничивающего поля суммарный вектор магнитного момента предмета может сначала несколько возрасти по модулю, а затем с ростом частоты намагничивающего поля будет уменьшаться, становясь заметно меньше значения, соответствующего нулевой частоте. Вследствие этого составляющая индуцированного магнитного момента, синфазная с намагничивающим полем, у ферромагнитного предмета меняет знак при возрастании частоты, а у

неферромагнитного не меняет. Квадратурная составляющая магнитного момента всегда имеет один и тот же знак для любого предмета. Это дает возможность различать эти предметы между собой.

Кроме типа материала на величину комплексного сопротивления катушки влияет расположение предмета относительно катушки. Зависимость этой характеристики катушки от перечисленных параметров соответственно по-разному влияет на амплитуду и фазу ЭДС, наведенной в ней под действием переизлученного поля. При включении такой катушки в соответствующую измерительную схему становится возможным выделение сигналов и оценка их параметров, наиболее характерных для обнаруживаемых ОП.

Амплитуда сигнала от переизлученного поля сильно зависит от расстояния между исследуемым предметом и катушками. Максимальный сигнал соответствует нахождению предмета вблизи приемной или излучающей катушки, а минимальный – позиции посредине между катушками.

Характерными признаками ОП при использовании импульсного намагничивания являются продолжительность и вид процесса затухания вихревых токов в обследуемом предмете, переносимые в сигнал, наведенный в приемной катушке переизлученным полем. За критерии селекции могут быть приняты текущие значения переходной характеристики для различных моментов времени или результат их совместной обработки по специальным алгоритмам распознавания ОП.

При применении этого метода идеальным является намагничивающее поле, изменяющееся по прямоугольному закону. Однако на практике получить это невозможно из-за электромагнитной инерции излучающей катушки. Ток в катушке, подключенной к генератору прямоугольных импульсов, будет нарастать по экспоненциальному закону с постоянной времени $\tau = L/R$.

При ограничениях на индуктивность L и активное сопротивление R ($L > 0{,}01$ Гн, $R > 5$ ом) постоянная времени τ составит не менее единиц миллисекунд, а длительность переднего фронта импульса намагничивающего поля составит $(3\ldots4)\tau$.

Задний фронт импульса намагничивающего тока зависит от быстродействия силовых ключей, разрывающих цепь этого тока, и еще в большей степени от условий отсутствия затухающих колебаний намагничивающего поля после выключения тока. При таких условиях длительность заднего фронта волны намагничивающего поля реально может составлять не менее 10^{-4} сек. Это значит, что при импульсном намагничивании в реальном металлодетекторе максимальная частота гармонических составляющих не может превысить 10 кГц. В настоящее время большое распространение получило импульсное намагничивание с формой волны поля в виде отрезков полусинусоид (или комбинация таких отрезков).

Кроме постоянной времени намагничивающей цепи (в обесточенном состоянии), необходимо учитывать и постоянную времени приемной катушки, воспринимающей поле переизлучения ОП. Для предотвращения

возникновения затухающих колебаний эта постоянная времени также должна быть не менее некоторого значения. Вследствие этого верхняя граница частотного диапазона поля переизлучения ОП при использовании метода переходных процессов, так же как и для намагничивающего поля, не превышает 10 кГц

Металлодетекторы подразделяются на переносные и стационарные, но принципы их работы одинаковы. Рассмотрим принципы работы индукционных токовихревых металлодетекторов на примерах переносных моделей [32].

Металлодетекторы низкой и сверхнизкой частоты. Здесь описываются детекторы «индуктивного баланса», которые иногда называют детекторами сверхнизкой частоты (СНЧ). Рабочая частота у таких детекторов ниже 30 кГц. В настоящее время это наиболее распространенная технология, включающая в себя также и детекторы низкой частоты (НЧ) – 30…300 кГц.

Внутри поисковой рамки металлодетектора низкой частоты (поисковую рамку также называют поисковой головкой, катушкой, антенной) располагается намотанный провод передающей катушки. Электрический ток, проходя по ней, создает переменное электромагнитное поле с частотой несколько килогерц.

При проходящем токе одного направления возникает магнитное поле, направленное в землю, а при смене направление тока магнитное поле будет направлено уже от земли (как южный и северный полюса у магнита). В любом металлическом или электропроводящем объекте, оказавшемся в зоне действия изменяющегося магнитного поля возникнут индуктированный электрический ток. Наведённый ток, в свою очередь, создаст собственное магнитное поле, направленное встречно магнитному полю передатчика.

Внутри рамки расположена еще одна (приемная) катушка, ориентированная таким образом, чтобы максимально ослабить взаимное влияние передающей катушки. Для этой цели используются и другие специальные методы. Электромагнитное поле от оказавшегося поблизости металлического предмета будет наводить в приемной катушке ЭДС и ток, который можно усилить и обработать электронными средствами, предварительно отфильтровав его от более мощного сигнала передатчика.

Принятый сигнал из-за электромагнитной инерции приемной катушки и объекта появляется с некоторым сдвигом по фазе относительно излученного сигнала. Максимальный фазовый сдвиг обеспечат объекты, которые обладают большей индуктивностью и меньшей резистивностью – это большие, толстые предметы, сделанные из хороших проводников, таких как золото, серебро и медь. Меньший фазовый сдвиг обеспечивают объекты, которые обладают меньшей индуктивностью и большей резистивностью – это более мелкие, более тонкие объекты либо предметы, выполненные из материалов с худшей проводимостью.

Некоторые ферромагнитные материалы, которые плохо проводят электрический ток или совсем его не проводят, из-за остаточной намагниченности также могут вызывать сильный сигнал в приемнике. В этом случае

сигнал в приёмнике покажет минимальный либо нулевой фазовый сдвиг. Многие типы почвы содержат мельчайшие крупинки железосодержащих минералов, которые на детекторе будут определяться как ферромагнетики.

Так как переизлученный от любого металлического предмета сигнал имеет свой определенный фазовый сдвиг, то можно селектировать различные типы объектов. Например, серебряная монета даёт значительно больший фазовый сдвиг, нежели алюминиевый предмет такого же размера, поэтому можно так настроить детектор, что он будет подавать звуковой или иной сигнал в первом случае и молчать во втором. Процесс идентификации металлических объектов называется дискриминацией. Самая простая форма дискриминации позволяет прибору подавать сигнал, когда рамкой проводят над объектом, фазовый сдвиг сигнала от которого превышает установленную среднюю величину. К сожалению, аппараты с таким типом дискриминатора не будут срабатывать на некоторые монеты и большую часть ювелирных изделий, если порог дискриминации установлен достаточно высоко для игнорирования мелких алюминиевых предметов.

Более совершенная схема – это так называемый дискриминатор с выделением диапазона (notch discriminator). Такого типа схемы реагируют на объекты в пределах определенного диапазона (например, диапазон «никелевые монетки и кольца») и не будут реагировать на фазовые сдвиги сигнала как выше этого диапазона (пуговицы, крышечки от лекарств), так и ниже него (железо, фольга). Более качественные детекторы этого типа можно настроить так, что для каждого из нескольких диапазонов он будет либо реагировать либо наоборот игнорировать сигналы фазового сдвига внутри него. Например прибор White's Spectrum XLT дает возможность программировать 191 вариант различных диапазонов [32].

Практически все металлодетекторы оборудованы визуальным индикатором дискриминации и имеют также и звуковую систему распознавания.

Тип металлического объекта можно предсказать по коэффициенту отношения его индуктивности к его собственной резистивности (по постоянной времени RL-цепи), определяющему фазовый сдвиг. Электронная схема, называемая фазовым детектором, может измерить этот фазовый сдвиг. Обычно используется по двум каналам *X* и *Y* два таких фазовых детектора, пиковые величины сигнала, на которых они производят измерения, сдвинуты друг относительно друга на 1/4 длины волны передатчика или на 90°. Третий демодулирующий канал, называемый каналом *G*, может быть настроен так, что его отклик на любой сигнал с постоянным фазовым сдвигом относительно импульсов передатчика (например, почва) может быть уменьшен до нуля независимо от амплитуды этого сигнала. Это необходимо для разделения двух составляющих сигнала – отклика от почвы и от объекта, и определения наиболее вероятного типа объекта.

Более совершенные металлодетекторы имеют микропроцессор для обработки сигналов этих трех каналов и определения типа обьекта. Соотно-

шение показаний каналов *X* и *Y*, вне зависимости от значения канала *G*, есть некоторое число. Можно найти это отношение с разрешением – лучше, чем 500 к 1 по всему диапазону встречающихся материалов, от феррита до чистого серебра. Сигнал от железных объектов зависит от их ориентации, поэтому численная характеристика может сильно меняться, когда рамка движется над ними. Графические дисплеи, откладывающие отношение *X*/*Y* по горизонтальной оси, а амплитуду принятого сигнала по вертикальной оси, очень полезны для отбраковывания металлического мусора от более ценных предметов. Такой тип дисплея называют «сигмаграфом» (SigmaGraph TM).

В режиме работы металлодетектора «все металлы» (без дискриминации сигналов по фазовому сдвигу) особенно важна хорошая отстройка от земли. Так как большинство почв являются железосодержащими, а также могут обладать электропроводностью из-за присутствия солей, растворенных в подпочвенной воде, то сигнал от почвы может быть в 1000 раз сильнее сигнала от зарытого в землю на достаточную глубину металлического предмета. Однако фазовый сдвиг принимаемого сигнала от почвы остаётся достаточно постоянным в пределах некоторой площади с однородными свойствами. Можно так сконструировать детектор, что даже когда сигнал от земли сильно изменяется (например, при поднимании и опускании рамки, или при прохождении оператора по насыпи или над ямой) показания металлодетектора будут оставаться неизменными. Эффективная отстройка от земли делает возможным определить с большой точностью как расположение объекта, так и оценить глубину его залегания. Возможна также «следящая отстройка от земли» (tracking ground balance). Хорошие детекторы с такой функцией позволяют настроившись раз, провести всю работу без дополнительных подстроек.

Металлодетекторы с импульсной индукцией. Устройство поисковой катушки или рамки металлодетектора с импульсной индукцией значительно проще по сравнению с СНЧ приборами. Одна и та же катушка с намотанным проводом используется как для передачи, так и для приема сигналов.

Передающая схема состоит из электронного (бесконтактного) ключа, который подключает катушку на короткое время на батарею питания. Сопротивление катушки очень мало, поэтому по катушке может протекать ток силой в несколько ампер. После подачи импульса тока в катушку электронный ключ затем обрывает его и затем опять включается для подачи следующего импульса. Скважность периодической последовательности импульсов, следующих с частотой от 22 Гц до нескольких килогерц, составляет обычно около 4%. Это исключает перегрев передатчика и катушки и уменьшает среднюю мощность, потребляемую от батареи. Чем ниже частота следования импульсов, тем больше может быть излучаемая мощность.

На более низких частотах достигается большая глубина и чувствительность обнаружения предметов, сделанных из серебра, но при этом падает

чувствительность к никелю и сплавам золота. Такие приборы имеют замедленную реакцию, поэтому требуют очень медленного перемещения рамки.

Более высокие частоты излучения повышают чувствительность к никелю и сплавам золота, но понижают чувствительность к серебру.

Передатчик действует подобно катушке зажигания автомобиля. Каждый импульс тока в передающей катушке создаёт магнитное поле. Когда ток достаточно быстро обрывается, магнитное поле вокруг катушки в таком же темпе исчезает, и в этот момент на катушке возникает импульс перенапряжения противоположной полярности и большой амплитуды. В металлодетекторах с импульсной индукцией амплитуда импульса перенапряжения ниже – обычно от 100 до 130 вольт в пике. По длительности импульс очень небольшой – 30 микросекунд. Он называется «отраженным импульсом».

От величины электрического сопротивления катушки с проводом зависит время затухания этого электрического импульса. Полное отсутствие сопротивления, или напротив – очень большая его величина заставит импульс «звенеть», т.е. иметь колебательный характер. При достаточном электрическом сопротивлении время затухания импульса укорачивается (уменьшается постоянная времени) и отраженный импульс «сглаживается». Чрезмерное или недостаточное подавление импульса будет вносить нестабильность в работу и маскировать хорошо проводящие металлы и уменьшать глубину обнаружения.

Если металлический предмет находится поблизости от поисковой катушки, то он запасает в себе часть энергии импульса, что приводит к затягиванию процесса затухания импульса до нулевого уровня. Изменение в ширине отраженного импульса свидетельствует о присутствии металлического объекта.

Для того чтобы выделить сигнал от объекта, необходимо измерить заднюю часть импульса, где он спадает до нуля (хвост). На входе приемника после катушки стоит амплитудный ограничитель, который ограничивает напряжение входного импульса до величины 1 вольт для исключения перегрузки измерительной схемы. Сигнал в приемнике состоит из импульса от передатчика и отраженного импульса. Усиленный сигнал от приемника поступает в схему измерения времени спадания импульса напряжения до нуля. Отраженный импульс преобразуется в последовательность импульсов (стробов) для удобства измерения времени спадания.

Далее стробированный сигнал преобразуется в напряжение постоянного тока. Это выполнятся накопительной схемой (интегратором), которая преобразует стробы в напряжение, пропорциональное их количеству. Напряжение возрастает, когда объект расположен близко от рамки и уменьшается при удалении от объекта. Напряжение дополнительно усиливается и управляет схемой звукового контроля.

Образцы металлодетекторов. Досмотрово-сигнальный комплекс АКА 7202М (рис. 3.25) обладает высокой чувствительностью (обнаруживает 5 мм обломок иглы) и высоким темпом сканирования за счет увеличенной площади датчика. Максимальная дальность обнаружения металлических объектов (на воздухе): фрагмент полотна для ручной ножовки длиной 150 мм – до 9 см, лезвие безопасной бритвы (немагнитная, нержавеющая сталь) – до 3 см [57].

Ручной металлодетектор ADAMS AD10-2 (рис. 3.25) обнаруживает черные и цветные металлы массой более 0,1 г, имеет ударопрочный корпус, сверхнадежный выключатель напряжения питания (до 10 млн. переключений). Осуществляет «селекцию по габаритам» – чем крупнее обнаруженный металлический предмет, тем длительнее звучание сигнала тревоги, а также световую и звуковую индикацию обнаружения [57].

Рис. 3.25. Досмотрово-сигнальные комплексы «АКА 7202М» и «ADAMS AD18»

Селективный обнаружитель оружия в ручной клади РУБЕЖ-Д (рис. 3.26) предназначен для контроля ручной клади посетителей (портфелей, дамских сумочек) в комплекте со стационарным металлодетектором или при автономной работе [57]. Может располагаться в непосредственной близости от стационарного металлодетектора, не реагирует на металлическую окантовку кейсов и сумочек, обеспечивает звуковую и световую сигнализацию.

Рис. 3.26. Компьютеризированный металлодетектор «КОРНЕТ» и селективный обнаружитель оружия в ручной клади «РУБЕЖ»

Вероятность ложных срабатываний от набора предметов личного пользования общей массой до 200 г – не более 0,05. Пропускная способность – до 60 предметов в минуту.

Профессиональный, компьютеризированный, селективный металлодетектор КОРНЕТ, модель 7250 (рис. 3.26) обеспечивает [57]:

- новейшую, не имеющую аналогов, технологию опосредованной визуализации объектов поиска в виде спектральных годографических образов на экране графического ЖК дисплея;
- мгновенный ввод в работу восьми пользовательских программ поиска;
- широкие программируемые возможности звуковой индикации, включая новейшую разработку – «режим PCO» (Phase Control Oscillator);
- автоматический и ручной баланс грунта.

Выпускается в двух вариантах исполнения: в пластмассовом (гражданская версия) и металлическом герметизированном корпусе (войсковая версия).

Дальность обнаружения металлических объектов (на воздухе) – от 45 до 250 см в зависимости от размеров предметов.

3.12. Портативная рентгенотелевизионная установка «НОРКА»

В рентгенотелевизионной установке «НОРКА» (рис. 3.27) использован модульный принцип построения. В состав установки могут входить как микрофокусные излучатели, так и сильноточные серии «РАП» [57].

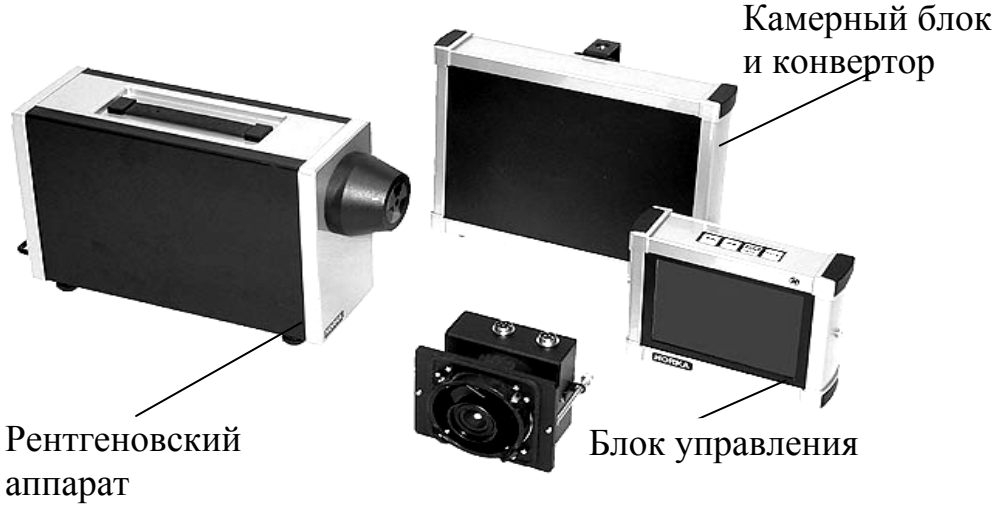


Рис. 3.27. Рентгенотелевизионная установка «НОРКА»

Досмотровая установка НОРКА комплектуется одним из блоков управления: «БУ-2М» или «БУ-4». Миниатюрный пульт «БУ-2М» снабжен монитором размером 6,4" и памятью на 150 изображений (с возможностью расширения до 1024), которые, при желании, могут быть переписаны в

персональный компьютер. В портативном компьютерном блоке управления «БУ-4» реализована возможность цифрового увеличения любого участка изображения. Программное обеспечение рентгена позволяет получать псевдоцветные изображения, производить цифровое улучшение изображений, архивирование рентгентелевизионных изображений, представлять изображения в негативном и позитивном изображениях, вносить речевые комментарии.

Система обнаружения «НОРКА» комплектуется блоком телекамеры, который устанавливается на один из трех сменных преобразователей. Выбор конкретного преобразователя обуславливается габаритами контролируемого объекта и требуемым пространственным разрешением. В комплект поставки досмотровой установки могут входить один, два, либо несколько преобразователей.

Основные достоинства системы «НОРКА»:

- быстрое развертывание на месте обследования;
- исключительная оперативность в работе;
- высокая производительность;
- хорошая выявляющая способность;
- исключение «мокрого» фотографического процесса, связанного с обработкой рентгеновских фотопленок;
- возможность записи теневых изображений, получаемых в результате просвечивания, в электронную память прибора для последующего анализа и обработки;
- возможность работы от аккумуляторной батареи

В системе обнаружения «НОРКА-XL» может быть реализован метод двуэнергетической цифровой радиографии (дуальной энергии), с помощью которого возможно классифицировать содержание досматриваемых объектов с определением принадлежности к классам «металл» или «не металл» с указанием относительной толщины материалов.

В состав комплекта досмотровой системы «НОРКА-МИНИ» входят:

- «БУ-2М» – Блок управления LCD-6,4"; 150 изображений
- «РИ-100М» – Рентгеновский излучатель острофокусный 100 кэВ
- «СКБ-2Д» – Цифровой сменный камерный блок (800×600 пикселей, 10 бит)
- «ПР-1» – Конвертер 114×152 мм
- «БАП-1/ЗУ» – Аккумуляторный блок питания в комплекте с зарядным устройством
- Специальное программное обеспечение

3.13. Досмотровые эндоскопы

На рис. 2.28 показан специальный досмотровый комплект эндоскопов, который предназначен для визуального осмотра труднодоступных, в том

числе светоизолированных, мест в технических системах в условиях отсутствия вблизи питающей электрической сети [47].

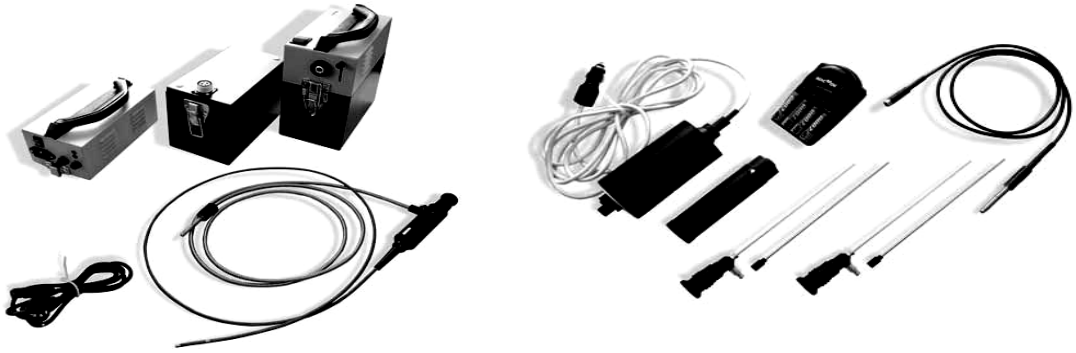


Рис. 3.28. Досмотровый комплект эндоскопов

Комплект содержит:

1. Эндоскопы технические жесткие ЭТЖ 2-2-0 и ЭТЖ 2-2-90.
2. Эндоскоп технический гибкий ГТЭ 6-1,5.
3. Осветитель с автономным питанием ОАК-2М.
4. Набор специального инструмента (рис. 2.29).

Рис. 3.29. Набор специального инструмента для эндоскопов

Технические характеристики комплекта:

Масса комплекта в полной комплектации – не более 14,0 кг.

Габаритные размеры:

– упаковочный чемодан для эндоскопов – 51×42×18 см.;

– упаковочный чемодан для инструмента – 49×42×16 см.

Масса комплекта эндоскопов – не более 8,5 кг.

Масса комплекта специального инструмента – не более 5,5 кг.

Суммарное время работы переносного блока осветителя без подзарядки – не менее 60 мин.

Длина осветительного кабеля – не менее 200 см.

Вопросы для самопроверки

1. Виды средств обнаружения радиозакладочных устройств.

1. Перечислите основные устройства выявления побочных электромагнитных излучений.

5. Перечислите известные Вам программно-аппаратные комплексы для измерения ПЭМИН.

6. Типовой состав автоматизированных комплексов радиомониторинга.

7. Технические возможности комплексов радиомониторинга.

8. Какие характеристики электромагнитного поля определяются в выявленных побочных электромагнитных излучениях?

9. В каких расчетах используются характеристики электромагнитного поля побочных электромагнитных излучений?

10. Принцип действия и назначение нелинейного локатора. Типы нелинейных локаторов.

11. Перечислите известные Вам комплексы для измерения характеристик акустических сигналов.

12. Какие устройства составляют основу комплексов для измерения характеристик акустических сигналов?

13. Какие характеристики помещений определяются при выявлении каналов утечки речевых сигналов?

14. Какие требования предъявляются к современным металлодетекторам?

15. Назначение досмотровых эндоскопов.

16. Какие досмотровые устройства применяются для выявления технических каналов утечки информации?

17. В каких случаях применяются рентгенотелевизионные устройства?

18. Особенности канала утечки речевой информации за счет акустоэлектрических преобразований.

4. СКРЫТИЕ И ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

4.1. Концепция и методы инженерно-технической защиты информации

Системы технической защиты

Концепция инженерно-технической защиты информации определяет основные принципы, методы и средства обеспечения информационной безопасности объектов. Она представляет собой общий замысел и принципы обеспечения информационной безопасности объекта в условиях угроз и включает в себя:

- оценку угроз;
- систему защиты информации;
- принцип построения системы защиты информации.

Инженерно-техническая защита представляет собой совокупность специальных органов, технических средств и мероприятий по их использованию для защиты конфиденциальной информации.

Эффективная техническая защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых затрат на организацию защиты информации. Техническая защита информации предполагает комплекс мероприятий по защите информации от несанкционированного доступа по различным каналам, а также нейтрализацию специальных воздействий на нее – уничтожения, искажения или блокирования доступа.

Цели и задачи технической защиты:

- предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;
- защита носителей информации от уничтожения в результате различных природных и техногенных воздействий;
- предотвращение утечки информации по различным техническим каналам.

Принципы проектирования систем технической защиты [39]:

- непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;
- многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;
- избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации;

• интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;

• создание централизованной службы безопасности в интегрированных системах.

По функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

• инженерные средства, представляющие собой различные устройства и сооружения, противодействующие физическому проникновению злоумышленников на объекты защиты;

• аппаратные средства (измерительные приборы, устройства, программно-аппаратные комплексы и др.), предназначенные для выявления каналов утечки информации, оценки их характеристик и защиты информации;

• программные средства, программные комплексы и системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

• криптографические средства, специальные математические и алгоритмические средства защиты компьютерной информации, передаваемой по открытым системам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая: физическую, правовую, организационную, экономическую, инженерно-техническую, программно-математическую защиту, информационно-аналитическое обеспечение и консультативную помощь.

К целям защиты информации относятся: предотвращение утечки, хищения, утраты, искажения, подделки информации и предотвращение других несанкционированных негативных воздействий.

Безопасная информационная деятельность требует наличия системы ее защиты – комплекса организационных, организационно-технических и технических мероприятий по обнаружению, предотвращению и ликвидации возникших угроз объекту.

Создание новой системы защиты или оценка эффективности существующей системы безопасности объекта начинается с анализа возможных угроз и оценки их реального появления. Основой для анализа является исследование объекта на наличие уязвимостей в защите, изучение расположения и особенностей инженерных конструкций, коммуникаций и т.п. На следующем этапе осуществляется выбор соответствующих методов и средств адекватной защиты.

При оценке вероятных угроз объекту должны учитываться угрозы здоровью и безопасности персонала; угрозы целости и сохранности матери-

альных ценностей и оборудования; безопасность информации, сохранность государственной или коммерческой тайны.

Для получения максимально реальной оценки угроз необходимы изучение и анализ статистических данных, связанных с попытками разведывательной деятельности на объекте в прошлом; оценка риска по каждому виду угроз; оценка ситуации на объекте и прилегающих к нему территориях на определенном интервале времени; изучение статистики по фактам разведдеятельности на подобных объектах.

Важным моментом в объективной оценке угроз и в разработке концепции защиты объекта является привлечение независимых экспертных организаций или специализированных государственных учреждений, имеющих квалифицированный персонал. В этом случае исключается субъективная оценка разведдоступности объекта и проводится квалифицированная разработка концепции защиты.

Несмотря на большое разнообразие возможных информационных угроз, проектирование защиты от каждой из них должно вписываться в комплексную систему защиты. Комплексная система защиты предусматривает надежное перекрытие всех опасных каналов утечки информации.

Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам оценивается по различным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы:

- скрытие;
- дезинформация.

К первой группе относятся:

- пассивное скрытие;
- активное скрытие;
- специальная защита.

Ко второй группе относятся:

- техническая дезинформация;
- имитация;
- легендирование.

Суть пассивного скрытия заключается в исключении или значительном затруднении обнаружения объектов, а также в ослаблении до необходимого уровня их демаскирующих признаков.

Пассивное скрытие состоит из организационных мероприятий и технических мер.

К организационным мероприятиям относятся:

- территориальное, пространственно-временное, энергетическое и частотное ограничения на функционирование объектов;

• затруднения для ведения технической разведки путем использования маскирующих свойств местности, местных предметов, времени суток;

• установление контролируемых зон в месте расположения скрываемых видовых объектов.

К техническим мерам пассивного скрытия относятся:

• снижение контрастности демаскирующих признаков скрываемых видовых объектов по отношению к фону;

• снижение уровня информационных физических полей, создаваемых функционирующим объектом;

• применение маскирующих покрытий для видовых объектов;

• камуфлирование техники;

• применение при настройке радиоэлектронной аппаратуры эквивалентов антенн, закрытых антенно-фидерных устройств, экранированных камер и сооружений, исключающих электромагнитные излучения в окружающее пространство.

Суть активного скрытия состоит главным образом в создании маскирующих шумовых помех различной физической природы техническим средствам разведки и в создании ложной обстановки по физическим полям скрываемого объекта.

Активное скрытие применяется в большинстве случаев как дополнительная мера к пассивному скрытию, когда не обеспечиваются условия снижения уровня физического поля до безопасного значения.

Спецзащита реализуется аппаратными, криптографическими и программными способами. К спецзащите относятся скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К принципам инженерно-технической защиты информации относятся [39]:

• надежность защиты информации;

• непрерывность защиты;

• скрытность защиты информации;

• рациональность защиты;

• многообразие способов защиты;

• комплексное применение различных способов и средств защиты;

• экономичность защиты.

4.2. Экранирование электромагнитных волн

4.2.1. Электромагнитное экранирование и развязывающие цепи

Для снижения наводок необходимо устранять или ослаблять до допустимых значений паразитные связи. В первую очередь ослабление паразит-

ных связей должно производиться прямым уменьшением паразитной емкости, взаимной индуктивности и паразитного сопротивления. Способы уменьшения паразитных связей в принципе несложны: размещение вероятных источников и приемников наводок на максимально возможном расстоянии друг от друга; уменьшение габаритов токонесущих элементов, обеспечивающих минимум паразитной связи (для получения минимальной взаимоиндуктивности катушек индуктивности их оси должны быть взаимно перпендикулярны); сведение к минимуму общих сопротивлений; изъятие посторонних проводов, проходящих через несколько узлов или блоков, которые могут связать элементы, расположенные достаточно далеко друг от друга; при невозможности исключения посторонних проводов, создающих паразитную связь, необходимо позаботиться о том, чтобы при емкостной паразитной связи сопротивление постороннего провода относительно корпуса было минимальным, при индуктивной паразитной связи необходимо увеличивать внутреннее сопротивление посторонней линии связи, в последнюю очередь – экранирование и развязывающие фильтры.

Экранирование – это локализация электромагнитной энергии в пределах определенного пространства путем преграждения ее распространения.

Развязывающий фильтр – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

Введение экранов часто требует существенного изменения компоновки, конструкции, а иногда и габаритов изделия, поэтому конструктор должен ясно понимать физическое действие каждой детали экрана, влияние любого элемента конструкции на значения паразитных связей. Желательно совмещать элементы экранов с элементами несущей конструкции. Общая рекомендация сводится к тому, что на начальном этапе конструирования необходимо принимать все возможные меры для снижения паразитных связей, а уж потом в ходе экспериментальной доводки изделия убрать те элементы, которые оказались лишними. Исключить какой-либо элемент из готового изделия почти всегда проще, чем добавить.

Экранирование электромагнитных волн является основой экологической безопасности и одним из самых действенных средств защиты объекта от утечки информации по техническим каналам.

В связи с бурно развивающейся техникой все острее становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и экологическую безопасность. Электромагнитная обстановка представляет собой совокупность электромагнитных полей в заданной области пространства, которая может влиять на функционирование конкретного радиоэлектронного устройства или биологического объекта.

Для создания благоприятной электромагнитной обстановки и для обеспечения требований по электромагнитной безопасности объекта, которая включает в себя и противодействие несанкционированному доступу к информации с использованием специальных технических средств, производится экранирование электромагнитных волн.

Применение качественных экранов позволяет решать многие задачи, среди которых защита информации в помещениях и технических каналах, задачи электромагнитной совместимости оборудования и приборов при их совместном использовании, задачи защиты персонала от повышенного уровня электромагнитных полей и обеспечение благоприятной экологической обстановки вокруг работающих электроустановок и СВЧ-устройств.

Под экранированием в общем случае понимается как защита приборов от воздействия внешних полей, так и локализация излучения каких-либо средств, препятствующая проявлению этих излучений в окружающей среде. В любом случае эффективность экранирования – это степень ослабления составляющих поля (электрической или магнитной), определяемая как отношение действующих значений напряженности полей в данной точке пространства при отсутствии и наличии экрана, Так как отношение этих величин достигает больших значений, то удобнее пользоваться логарифмическим представлением эффективности экранирования:

$$K_E = 20\lg\frac{E_0}{E_1},\ \text{dB},$$
$$K_H = 20\lg\frac{H_0}{H_1},\ \text{dB}, \qquad (4.1)$$

где K_E – коэффициент ослабления (экранирования) по электрической составляющей, K_H – коэффициент ослабления (экранирования) по магнитной составляющей, $E_0(H_0)$ – напряженность электрической (магнитной) составляющей поля в отсутствии экрана, $E_1(H_1)$ – напряженность электрической (магнитной) составляющей поля при наличии экрана в той же точке пространства.

Теоретическое решение задачи экранирования, определение значений напряженности полей в общем случае чрезвычайно затруднительно, поэтому в зависимости от типа решаемой задачи представляется удобным рассматривать отдельные виды экранирования: электрическое, магнитостатическое и электромагнитное. Последнее является наиболее общим и часто применяемым, так как в большинстве случаев экранирования приходится иметь дело либо с переменными, либо с флуктуирующими и реже – действительно со статическими полями.

Теоретические и экспериментальные исследования ряда авторов показали, что форма экрана незначительно влияет на его эффективность. Глав-

ным фактором, определяющим качество экрана, являются радиофизические свойства материала и конструкционные особенности. Это позволяет при расчете эффективности экрана в реальных условиях пользоваться наиболее простым его представлением: сфера, цилиндр, плоскопараллельный лист и т.п. Такая замена реальной конструкции не приводит к сколько-нибудь значительным отклонениям реальной эффективности от расчетной, так как основной причиной ограничивающей достижение высоких значений эффективности экранирования является наличие в экране технологических отверстий (устройства ввода-вывода, вентиляции), а в экранированных помещениях – устройств жизнеобеспечения, связывающих помещение с внешней средой.

Плоскопараллельный экран в электромагнитном случае можно характеризовать нормальным импедансом материала экрана, который определяется как отношение тангенциальных составляющих электрического и магнитного полей. Коэффициент прохождения через слой представляет собой эффективность экранирования, так как равен отношению амплитуд прошедшей и падающей на экран волны. Если средой по обе стороны экрана является вакуум, то коэффициент прохождения D можно представить в виде [3]

$$D=\frac{4Z_m}{(1+Z_m)^2 e^{-j\alpha d}-(1-Z_m)^2 e^{j\alpha d}}, \qquad (4.2)$$

$$Z_m=\sqrt{\frac{\mu_m}{\varepsilon_m}}, \qquad \alpha=\frac{2\pi}{\lambda_0}\sqrt{\varepsilon\mu},$$

λ_0 – длина волны в свободном пространстве, а ε_m и μ_m – относительные диэлектрическая и магнитная проницаемости материала экрана.

В общем случае при комплексных диэлектрической и магнитной проницаемостях материала теоретический анализ приведенного выражения крайне затруднителен, поэтому большинство исследователей прибегают к раздельному рассмотрению эффективности экранирования – по поглощению и отражению падающей волны экраном.

Поскольку аналитическая оценка эффективности экранирования из общей формулы коэффициента прохождения для плоскопараллельного бесконечного экрана в общем случае сложна, то может быть использован более простой, приближенный анализ, основанный на представлении эффективности экрана как суммы отдельных составляющих:

$$K=K_{\text{погл}}+K_{\text{отр}}+K_{\text{н.отр}}, \qquad (4.3)$$

где $K_{\text{погл}}$ – эффективность экранирования вследствие поглощения экраном электрической энергии, $K_{\text{отр}}$ – эффективность экранирования за счет отражения электромагнитной волны экраном, $K_{\text{н.отр}}$ – поправочный коэффици-

ент, учитывающий многократные внутренние переотражения волны от поверхностей экрана.

Если потеря энергии волны в экране, то есть ее поглощение, превосходит 10 дБ, то последним коэффициентом в приведенном выражении можно пренебречь. Эффективность экранирования вследствие поглощения энергии в толще экрана можно рассчитать из простого соотношения $K_{\text{погл}} = 8{,}7d\sqrt{\pi f \mu_m \sigma}$, полученного на основе представления электрической и магнитной составляющей поля в материале, на поверхности которого выполняются граничные условия Леонтовича.

4.2.2. Подавление емкостных паразитных связей

Емкостная паразитная связь между двумя электрическими цепями возникает через ближнее электрическое поле. Для снижения паразитной емкости между электрическими цепями вводится токопроводящий экран, соединенный с общим проводом и замыкающий на общий провод большую часть электрических силовых линий [3].

Введением экрана, имеющего сопротивление, равное нулю относительно общего провода, теоретически наводку можно снизить до нуля. Практически же всегда из-за наличия проводников и технологических отверстий и возникновения краевых эффектов имеется остаточное ближнее электрическое поле и, следовательно, остаточная емкость.

При экранировании электрического поля очень важно создать низкое сопротивление экрана относительно корпуса (общего провода). Появление любого сопротивления, особенно индуктивного, в цепи соединения экрана с общим проводом создает эффект паразитной связи через посторонний провод, поэтому все металлические элементы конструкции всегда должны тщательно соединяться между собой и с общим проводом.

4.2.3. Подавление индуктивных паразитных связей

Паразитная индуктивная связь возникает между двумя электрическими цепями через ближнее магнитное поле. Для снижения величины магнитных полей используют два вида экранирования: магнитостатическое и динамическое.

Магнитостатическое экранирование или экранирование шунтированием магнитного поля основано на применении экранов из ферромагнитных материалов с большой магнитной проницаемостью. Линии магнитного поля как бы втягиваются в материал с более высокой магнитной проницаемостью, в результате внутри экрана поле ослабляется. Эффективность магнитостатического экранирования зависит от магнитного сопротивления экрана [3]

$$Э = 1 + \mu h / D, \qquad (4.4)$$

где μ – относительная магнитная проницаемость; h – толщина стенок экрана; D – диаметр эквивалентного сферического экрана. Для экрана в форме куба D = l,2b; b – размер стороны куба.

Эффективность магнитостатического экранирования не зависит от частоты в тех пределах, в которых от частоты не зависит магнитная проницаемость материала экрана. Эффективность экранирования снижается при наличии в конструкции экрана стыков и швов, идущих поперек линий магнитного поля и снижающих эффективное значение магнитной проницаемости экрана. Магнитостатическое экранирование имеет невысокую эффективность: $Э$ =2÷5; им пользуются в основном на низких частотах, на которых мала эффективность динамического экранирования.

Сущность динамического экранирования заключается в том, что переменное магнитное поле ослабляется по мере проникновения в металл, так как внутренние слои экранируются вихревыми токами, возникающими в слоях, расположенных ближе к поверхности. Экранирующее действие вихревых токов определяется двумя факторами: обратным полем, создаваемым токами, протекающими в экране, и поверхностным эффектом в материале экрана. Вследствие экранирования внутренних слоев вихревыми токами, циркулирующими в поверхностных слоях, переменное магнитное поле ослабляется по толщине материала экрана. Это вызывает неравномерное распределение токов по толщине экрана, называемое поверхностным эффектом:

$$I_x / I_n = e^{-x/\delta}, \qquad (4.5)$$

где $I_x, I_п$ – плотность тока на глубине x и на поверхности экрана; $\delta = 2\sqrt{\rho/(2\mu\mu_0\omega)}$ – эквивалентная глубина проникновения тока, на которой плотность тока ослабляется в e раз; ρ – удельное сопротивление материала экрана, Ом×м; μ – относительная магнитная проницаемость; μ_0 – абсолютная магнитная проницаемость вакуума; ω – круговая частота.

На частотах, на которых толщина $h > \delta$, действуют оба фактора, и эффективность экранирования

$$Э = e^{x/\delta}\left(\frac{1}{2} + \frac{D}{\delta \cdot 2{,}8 \cdot K_ф \mu}\right), \qquad (4.6)$$

где h – толщина стенок экрана; D – ширина прямоугольного экрана или диаметр цилиндрического; $K_ф$ – коэффициент формы. Для прямоугольного экрана $K_ф = 1$, цилиндрического $K_ф = 2$, сферического $K_ф = 3$.

На очень высоких частотах, где $h >> \delta$, величина в скобке всегда больше 0,5, что позволяет упростить выражение (4.6) как

$$Э \geq 0{,}5 e^{h/\delta}. \qquad (4.7)$$

Из (4.7) проще получить формулу для расчета минимальной толщины стенок экрана, обеспечивающей эффективность экранирования не ниже заданной:

$$h \geq \delta \ln 2Э. \qquad (4.8)$$

На низких частотах или при малой толщине стенок экрана ($h>\delta$) влияние поверхностного эффекта ниже, и эффективность экранирования определяется как

$$Э = \sqrt{1+[\omega\mu_0 Dh/(2K_ф\rho)]^2}. \qquad (4.9)$$

4.2.4. Экранирование проводов и катушек индуктивности

При экранировании реальных элементов, например трансформаторов, катушек индуктивности, проводов и т. д., обычно требуется одновременное экранирование от электрических и магнитных полей [3]. Желательно в качестве электрических и магнитных экранов использовать одни и те же элементы конструкции, но при этом следует учитывать, что действуют они поразному. Токи, протекающие по экрану под действием высокочастотного магнитного поля, во много раз больше токов, возникающих под действием электрического поля, поэтому эффективность электрического экрана практически не зависит от проводимости материала экрана, его магнитной проницаемости и частоты колебаний электрического поля. На эффективность магнитного экрана влияют проводимость, магнитная проницаемость и частота колебаний магнитного поля. Эффективность магнитного экранирования не зависит от наличия контакта с общим проводом, эффективность электрического экрана однозначно определяется наличием хорошего электрического соединения с общим проводом. Для одновременного экранирования электрического и магнитного полей необходимо выполнить обе группы требований.

При экранировании катушек индуктивности следует также учитывать влияние экрана на индуктивность и добротность. Чем ближе расположен экран к катушке индуктивности, тем больше потери, вносимые экраном, и сильнее снижаются добротность и индуктивность. Потери, вносимые экраном, возрастают с увеличением удельного сопротивления и уменьшением расстояния между экраном и катушкой. Поэтому при разработке экранов высокочастотных катушек желательно выбирать материалы с малым сопротивлением (медь, латунь, алюминий). Размеры экрана рекомендуется выбирать таким образом, чтобы зазор между катушкой и экраном был не менее $0{,}5d_{кат}$, т.е.

$$D_{эк} \geq 2d_{кат};\ \ l_{эк} \geq l_{кат} + d_{кат}, \qquad (4.10)$$

где $l_{кат}, d_{кат}$ – длина и диаметр намотки катушки; $l_{эк}, D_{эк}$ – высота и диаметр экрана.

Толщину стенок – экрана выбирают в соответствии с (4.8).

При размещении высокочастотной катушки индуктивности в экране с размерами в соответствии с (4.10) снижается ее индуктивность на 15–18%, если размеры катушки укладываются в соотношении $3d_{\text{кат}} > l_{\text{кат}} > d_{\text{кат}}$, то при этом возникают дополнительные потери, вносимые экраном,

$$\xi \approx 3 \cdot 10^{-4} \sqrt{f_0 \rho_{\text{эк}} / (f \rho_{\text{м}})}, \qquad (4.11)$$

где $f_0 = 1$МГц; f – рабочая частота; $\rho_{\text{м}}$ – удельное сопротивление меди; $\rho_{\text{эк}}$ – удельное сопротивление материала экрана [3].

Фактически получаемая эффективность экранирования обычно меньше рассчитанной по (4.6) и (4.7) за счет паразитной связи, возникающей через провода, выходящие из экранируемого пространства, и при наличии отверстий в экранах. Чтобы снижение эффективности было минимальным, отверстия для выводов должны быть расположены таким образом, чтобы не мешали вихревым токам: отверстия и вырезы в экране необходимо делать вытянутыми вдоль направления вихревых токов.

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), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или обеих сторон медной фольгой). Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. 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 отраженного 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 (триаксиальные 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.

Длина экранированного провода должна быть меньше четверти длины самой короткой волны спектра сигнала, иначе его надо рассматривать как длинную линию, которую надо нагружать на волновое сопротивление. Для уменьшения взаимного влияния длину монтажных цепей следует выбирать наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а не экранированные провода высокочастотных цепей – при пересечении под прямым углом.

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 однослойные и многослойные.

Материал: свинец, сталь, медь, алюминий или их сочетание.

В области низких частот корпуса многоштырьковых низкочастотных разъемов являются экранами и должны быть надежно заземлены.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению и иметь высокочастотные разъемы.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их в экранирующем распределительном коробе.

Для полного экранирования проводов от электрических и магнитных полей необходимо добиваться, чтобы весь обратный ток протекал по экрану, т.е. чтобы токи, протекающие по экранируемому проводу и экрану, были равны между собой (рис. 4.1, *а*). Для этого необходимо выводы генератора и нагрузки подключать к проводу и экрану непосредственно без промежуточных проводников, а соединение с корпусом производить в одной точке, лучше со стороны приемника сигнала. При подключении общего провода генератора к корпусу, а не к экрану (рис. 4.1, *б*) получается экранирование только от электрических полей. При отсутствии соединения экрана с общим проводом никакого экранирующего эффекта не возникает [3].

При соединении экрана с корпусом со стороны генератора или при соединении с корпусом через длинный провод эффективность экранирования падает за счет появления напряжения помех на этом проводе. Для экранирования проводов от низкочастотных наводок поверх экрана должна иметься изолирующая оболочка, исключающая случайные контакты с металлическими элементами корпуса изделия.

При замыкании экрана на корпус (рис. 4.1, *в*) нарушается магнитное экранирование части провода, расположенного между точкой замыкания экрана на корпус и нагрузкой. В этом случае довольно часто наблюдается, что при отключении соединения экрана около нагрузки уровень наводок снижается.

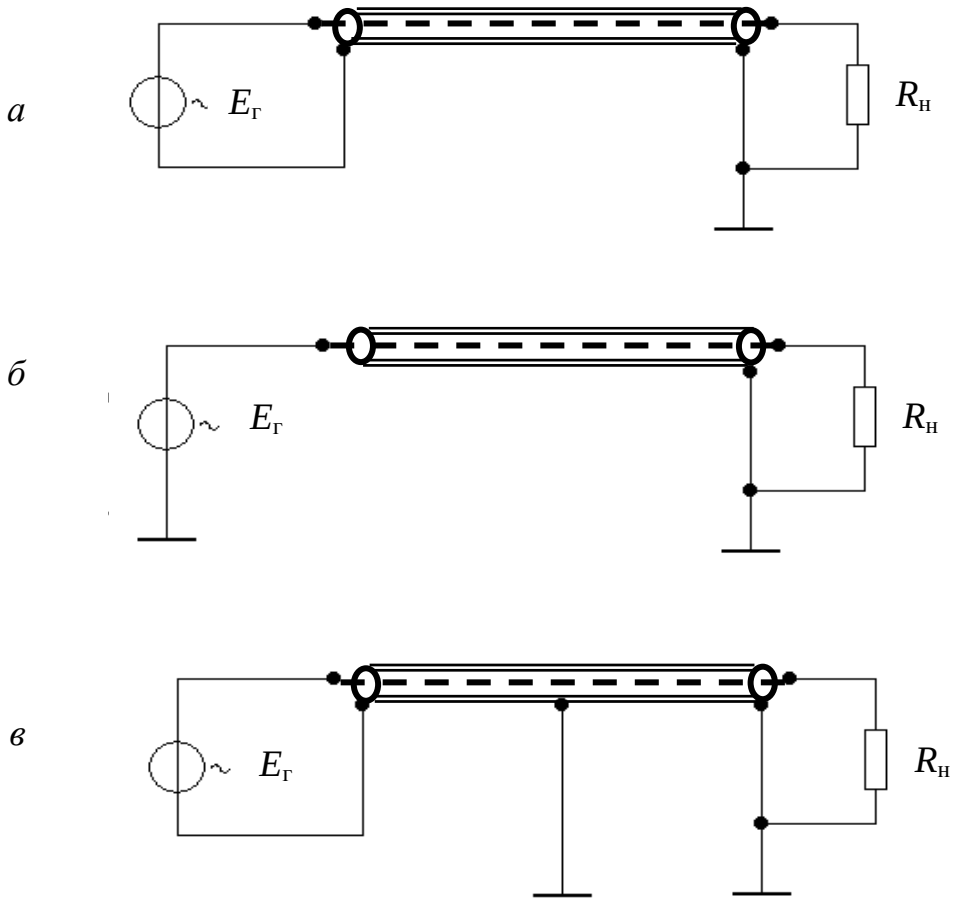


Рис. 4.1. Полное экранирование провода от электрических и магнитных полей (*а*), экранирование провода от электрических полей (*б*) и замыкание части экрана провода на корпус (*в*)

Если это явление наблюдается, необходимо найти и устранить замыкание экрана на корпус.

На высоких частотах из-за поверхностного эффекта обратный ток протекает в основном по внутренней поверхности экрана, поэтому на частотах более 10 МГц замыкание экранов на корпус не снижает эффективности экранирования.

При конструировании всегда необходимо учитывать, что при применении экранированных проводов резко увеличиваются габариты, стоимость и паразитная емкость монтажа, поэтому применять экранированные провода и коаксиальные кабели необходимо только в том случае, когда другие средства не дали нужного эффекта.

Очевидно, что на низких частотах стальной экран, магнитная проницаемость которого может быть достаточно высока (или экран из другого электропроводящего материала со значительной магнитной проницаемостью), оказывается эффективнее медного по поглощению. Однако для повышения его эффективности приходится увеличивать толщину экранирующего листа. Кроме того, с ростом частоты магнитная проницаемость

всех материалов быстро уменьшается, причем тем значительнее, чем больше ее начальное значение. Поэтому материалы с большим значением начальной магнитной проницаемости (104 Гн/м) целесообразно использовать только до частот порядка 1 кГц. При больших значениях напряженности магнитного поля из-за насыщения материала ферромагнетика его магнитная проницаемость падает тем резче, чем больше начальное значение проницаемости.

Во избежание эффекта насыщения экран делают многослойным, при этом желательно, чтобы каждый последующий (по отношению к экранируемому излучению) слой имел большее начальное значение магнитной проницаемости, чем предыдущий, так как эквивалентная глубина проникновения электромагнитного поля в толщу материала δ обратно пропорциональна произведению его магнитной проницаемости и проводимости. Толщина экрана d, необходимая для обеспечения заданного значения его эффективности, легко определяется из выражения $K = 8{,}7d/\delta$.

Вторая составляющая эффективности экранирования в (4.3) $K_{\text{отр}}$ обусловлена отражением электромагнитной волны на границе раздела «свободное пространство – экран» из-за различия волновых сопротивлений вакуума (Z для ближних полей – электрического или магнитного и Z для полей дальней зоны).

Эффективность экранирования вследствие отражения можно просто определить как $K = 20\log Z_m/4Z$, где Z для металлических материалов можно представить в виде:

$$Z \approx \sqrt{\frac{2\pi f \mu_m}{\sigma}} \text{ или } Z \approx \frac{\sqrt{2}}{\sigma\delta}. \qquad (4.12)$$

Значительно большего эффекта экранирования можно достичь, используя не однородные, а многослойные экраны той же суммарной толщины. Это объясняется наличием в многослойных экранах нескольких границ раздела поверхностей, на каждой из которых происходит отражение электромагнитной волны вследствие разницы волновых сопротивлений слоев. Эффективность многослойного экрана зависит не только от числа слоев, но и порядка их чередования. Наиболее эффективны экраны из комбинаций магнитных и немагнитных слоев, причем наружный по отношению к источнику излучения поля слой предпочтительнее выполнять из материала, обладающего магнитными свойствами.

Расчет эффективности экранирования двухслойными экранами из различных материалов показывает, что наиболее целесообразным в диапазоне частот 10 кГц – 100 мГц является сочетание медного и стального слоев. При этом толщина магнитного слоя должна быть больше, чем немагнитного (сталь – 82% общей толщины, медь – 18%).

Дополнительное увеличение толщины экрана на один слой приводит к не очень заметному повышению эффективности экранирования.

При проектировании электромагнитных экранов в общем случае необходимо иметь в виду, что на сравнительно низких частотах наиболее сложно обеспечить эффективное экранирование магнитной составляющей поля, в то время как экранирование электрической составляющей не представляет особых трудностей даже при использовании перфорированных или сетчатых экранов.

Несмотря на то что на низких частотах высокопроводящие материалы могут обеспечить очень большие значения эффективности экранирования, в ряде случаев (по технологическим, конструктивным, экономическим соображениям) оказывается более целесообразным применять (особенно при экранировании статических и флуктуирующих магнитных полей с невысоким значением напряженности) магнитные материалы с высокими значениями начальной магнитной проницаемости. Для однослойного цилиндра, длина которого существенно превосходит его диаметр D_0 , эффективность экранирования составляющей напряженности магнитного поля: перпендикулярной оси цилиндра, может быть приближенно оценена как

$$K = 20\lg(1+\mu d/D_0)\,. \qquad (4.13)$$

Как и в электромагнитном случае, многослойные оболочки оказываются эффективнее однослойного экрана, причем их эффективность растет практически пропорционально числу слоев.

Особое место в ряду материалов, применяемых для экранирования статических и квазистатических магнитных полей, занимают аморфные ферромагнетики. Магнитные экраны изготавливают из сплавов типа пермаллоя с содержанием 20% железа и 80% никеля. Высокие магнитные свойства (большое значение μ_m и коэффициента экранирования) достигаются после сложной и дорогой термической обработки. Однако свойства экранов, изготовленных из таких материалов, изменяются под влиянием механических воздействий. Экраны, изготовленные из аморфных сплавов, не чувствительны к ударам и изгибам. Магнитные свойства аморфных сплавов достаточно высоки, что позволяет применять их в качестве материала экрана. Они обладают высокой начальной магнитной проницаемостью, которая сохраняет свой уровень до частот порядка сотен мегагерц. Например, для экранирования кабелей в аппаратуре, установленной на борту космических кораблей класса «Вояджер», использовалась ткань «Метшильд», изготавливаемая из аморфного сплава в виде ленты шириной 1,5 мм и толщиной 58 мкм. Результаты исследований показали, что экранирующая способность такой ткани достигает 11 дБ при напряженности магнитного поля 40 А/м и 24 дБ при напряженности поля 200 А/м при частоте 60 Гц. Эти значения превосходят характеристики для аналогичных эк-

ранов из пермаллоя в 1,5–2 раза и не меняются после механических воздействий.

На сегодняшний день для индустриальных помех и радиочастотного диапазона нашим специалистам удалось создать из аморфных сплавов экраны с коэффициентами экранирования до 60 дБ. Из аморфных ферромагнетиков также разработаны магнитные экраны для квазистатических полей (магнитного поля земли). Для магнитного экранирования малых объемов теперь возможно применение аморфного ферромагнитного микропровода.

Во многих случаях достаточно эффективным является использование неэкранированной витой пары. Экранированный многопарный кабель не обладает сколько-нибудь существенными преимуществами перед неэкранированным ни в скорости передачи данных, ни в устойчивости к внешним электромагнитным наводкам большой интенсивности, но, тем не менее, производится промышленностью. Кроме того, при использовании экранированного кабеля возникает серьезная проблема с заземлением экранной оплетки, заключающаяся в том, что симметричная конструкция кабеля не позволяет присоединять экранную оболочку кабеля напрямую к земле, как это делается в коаксиальных линиях связи. Экранная оболочка кабеля в данном случае не так полезна, как может показаться на первый взгляд, более того, экранная оболочка является носителем самой внушительной части энергии синфазной составляющей симметричной линии связи. Использование экранированного кабеля создает очевидную проблему: как и куда должна быть присоединена экранная оболочка кабеля, и как нейтрализовать ток синфазной составляющей протекающий по оплетке.

Простое заземление экранной оболочки кабеля не имеет никакого смысла, так как не устраняет проблемы проникновения синфазной помехи, и возникновения опасных потенциалов на входах микросхем.

Для подавления синфазных помех существует метод, основанный на применении индуктивно связанных катушек, размещенных на общем сердечнике (рис. 4.2). Катушки индуктивности, включенные по такой схеме, называют продольным трансформатором. Встречно включенные катушки индуктивности не оказывают никакого влияния на полезный сигнал в линии $I_{\text{вх}}$, как и на противофазную составляющую помехи. Для синфазной составляющей $I_{\text{син}}$ продольный трансформатор в идеале представляет собой бесконечно большое сопротивление.

При включении связанных индуктивностей в линию связи каждая обмотка катушки включается последовательно с соответствующим проводником. Фазировка катушек при этом должна быть такова, чтобы магнитные потоки обмоток (Φ_1 от полезного сигнала и противофазной помехи и Φ_2 от синфазной помехи) были противоположно направлены и соответственно

взаимно компенсированы для полезного сигнала и суммировались для синфазной помехи.

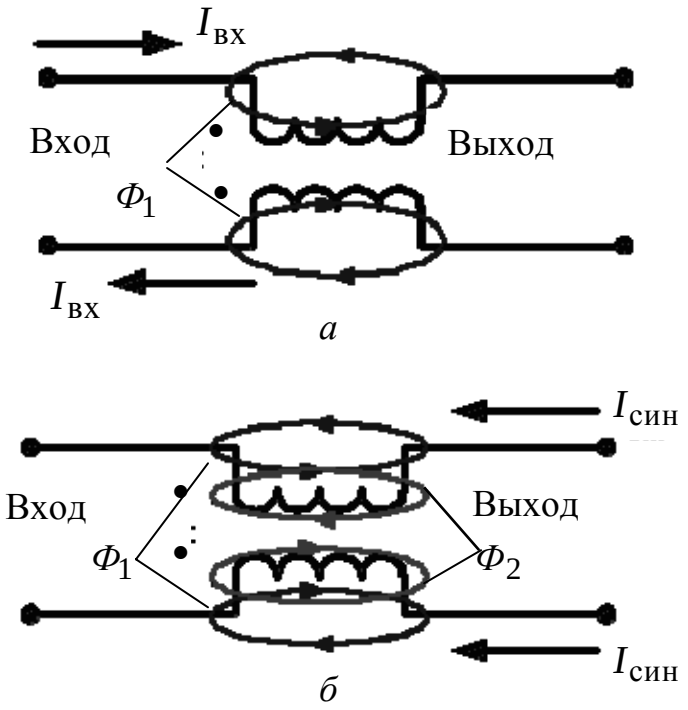


Рис. 4.2. Реакции продольного трансформатора: *а* – на полезный сигнал, *б* – на противофазную и синфазную помехи

Теоретически подавление синфазной помехи происходит полностью. Магнитные устройства такого типа называют продольным трансформатором.

Тороидальные сердечники обеспечивают большие значения индуктивности при заданных токах без применения зазора, и более эффективны на низких частотах.

Таким образом, применение продольных трансформаторов значительно уменьшает уровень синфазных помех в каналах передачи данных по витой паре.

4.2.5. Экранированные помещения

Экранироваться могут не только отдельные блоки аппаратуры и их соединительные линии, но и помещения в целом (рис. 4.3).

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующее свойство 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.

Схема экранированного помещения

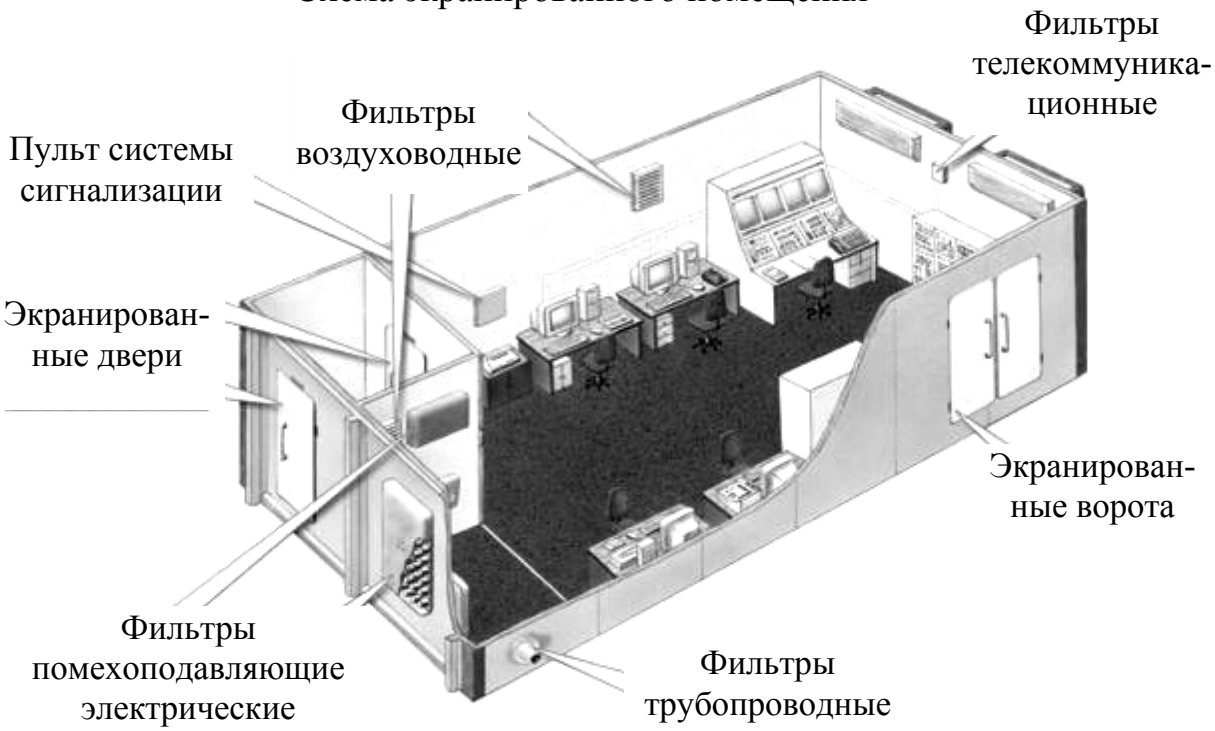


Рис. 4.3. Экранированное помещение

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах (рис. 4.3), в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Таким образом, экранированием электромагнитных волн возможно полностью обеспечить электромагнитную безопасность объекта. Однако обеспечение требований по электромагнитной безопасности объекта, особенно в части, касающейся защиты информации от утечки по техническим каналам, созданным с применением специального оборудования (электроакустический канал, радиоканал, канал побочных электромагнитных излучений и наводок и т.д.), необходимо предусматривать на стадии разработки проекта объекта. Так, например, при проектировании в пределах объекта необходимо выделить зоны повышенной конфиденциальности – комнаты переговоров, технологические помещения, в которых циркулирует информация, предназначенная для служебного пользования, и т.п. В таких помещениях не должно быть окон, они должны иметь независимую систему электропитания, экранированные двери. При строительстве такого объекта возможно применение экранирующих материалов – шунгитобетона или бетона с электропроводящим наполнителем. Стены помещения отделываются гибкими экранами, например тканными коврами из аморфных материалов или электропроводящими тканями. В качестве экранирующей ткани

возможно применение различных углетканей или металлизированных пленок.С внутренней стороны помещение облицовывается конструкционным радиопоглощающим материалом для предотвращения образования стоячих электромагнитных волн с частотами более 1 ГГц и для создания более комфортной экологической обстановки. В качестве радиопоглощающих материалов могут быть использованы специализированное пеностекло различных марок или сотовые конструкции. Коэффициент экранирования такого помещения может превышать 60 дБ в широком диапазоне частот.

Технологии позволяют производить качественное экранирование и уже существующих помещений, изначально не предназначавшихся для специального использования. Отделка стен многослойными гибкими экранами применима в большинстве случаев. При наличии окон они закрываются металлизированными пленками и шторами из экранирующих тканей. В помещениях такого класса возможно применение гибких широкодиапазонных радиопоглощающих материалов. Для облицовки потолков помещения применяется наполненное пеностекло. Коэффициент экранирования достигает значения 20 дБ и больше.

Мобильные экранированные сооружения выполняются как перевозимые контейнеры на любом виде соответствующего транспорта (рис. 4.4).

Рис. 4.4. Мобильное экранированное сооружение

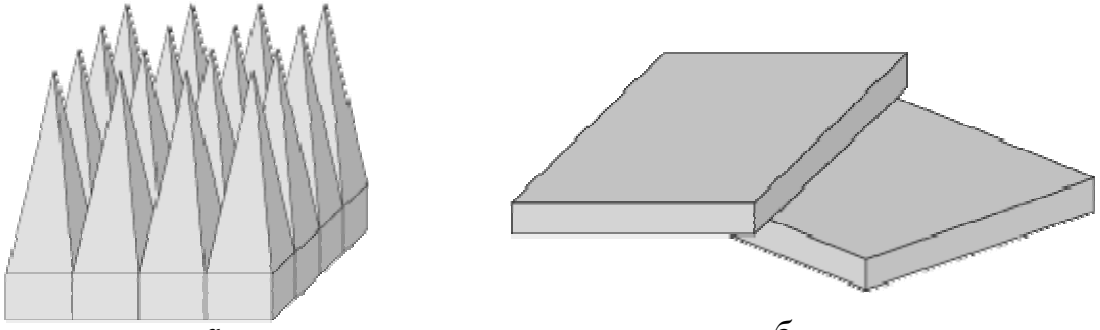
Безэховые камеры (БЭК) предназначены для проведения испытаний и высокоточных измерений радиоэлектронной аппаратуры, антенной техники и испытаний технических средств на электромагнитную совместимость. Обеспечивают получение достоверных результатов измерений в обстановке сильного электромагнитного зашумления естественным и техногенным электромагнитным фоном, а также могут использоваться как дополнительное средство защиты информации.

Существуют два основных типа безэховых камер – полубезэховая и полностью безэховая.

Полубезэховая камера – это экранированное помещение, у которого стены и потолок покрыты радиопоглощающим материалом. Абсорбирующие материалы присутствуют только на стенах и потолке, но пол остается отражающим (для испытаний на излучения). В полубезэховых камерах дополнительная установка радиопоглощающего материала на полу камеры позволяет обеспечить требуемую степень однородности испытательного поля на всех частотах.

Полностью безэховая камера – это экранированное помещение, у которого все внутренние поверхности покрыты абсорберами, радиопоглощающим материалом покрыт также пол. Покрытие камеры радиопоглощающим материалом преследует цель предотвратить отражения радиоволн от внутренних поверхностей камеры, так как интерференция отраженного и излученного электромагнитных полей может привести к образованию пиков и провалов напряженности результирующего электромагнитного поля. Этот тип безэховой камеры соответствует свободному пространству. Приемная антенна остается на фиксированной высоте.

Пирамидальный радиопоглощающий материал «Универсал-Дельта» (рис. 4.5, *а*) предназначен для облицовки потолков, стен, полов высококачественных универсальных безэховых камер и экранированных помещений, которые обеспечивают в широком диапазоне частот проведение высокоточных измерений параметров радиоэлектронной аппаратуры, антенной техники и технических средств на электромагнитную совместимость.



а *б*

Рис. 4.5. Поглотители электромагнитных волн:
а – пирамидальный поглотитель электромагнитных волн «Универсал–Дельта»;
б – плита базальтовая радиопоглощающая «Защита»

Поглотитель электромагнитных волн «Универсал-Дельта» конструктивно представляет собой пирамидальный тонкостенный контейнер, выполненный из трудногорючего материала и заполненный негорючей радиопоглощающей композицией с использованием углеродного волокна, что обеспечивает стабильность радиотехнических и эксплуатационных характеристик изделия.

Плита базальтовая радиопоглощающая «Защита» (рис. 4.5, *б*) представляет собой плоскую, жёсткую плиту, выполненную на основе базальтовых и углеродных волокон с неорганическим связующим материаллом.

Уровень безэховости зависит в основном от коэффициента отражения используемого материала и габаритов помещения.

4.3. Безопасность оптоволоконных кабельных систем

Важнейшими характеристиками волоконно-оптических систем передачи информации (ВОСПИ) являются [23]:

- слабое затухание сигнала и его меньшая зависимость от длины волны передаваемого информационного оптического сигнала, распределения мод и температуры кабеля;
- слабое искажение сигнала и его незначительная зависимость от спектральной ширины, распределения мод, амплитуды и длины волны передаваемого информационного оптического сигнала, длины световода и температуры окружающей среды;
- малые потери на излучение и их незначительная зависимость от радиуса изгиба и температуры волоконного световода;
- более приемлемые физические параметры – вес, размер, общий объем;
- простота укладки, сращивания и ввода излучения в световод;
- высокая устойчивость к внешним воздействиям – влагостойкость, теплостойкость, стойкость к химической коррозии и к механическим нагрузкам.

Несмотря на перечисленные преимущества, ВОСПИ характеризуются также недостатками, главным из которых является возможность утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН) как в радиочастотном, так и в оптическом диапазонах.

Оптоволокно – это обычное стекло, передающее электромагнитную энергию в инфракрасном диапазоне волн. Излучение наружу практически не просачивается. Эффективный перехват информации возможен только путем физического подключения к оптоволоконной линии. Однако если ВОСПИ рассматривать как систему, содержащую рабочие станции, серверы, интерфейсные карты, концентраторы и другие сетевые активные устройства, которые сами являются источником излучений, то проблема утеч-

ки информации становятся актуальной. Поэтому, принимая решения об использовании оптоволоконных кабельных систем (ОКС), необходимо учитывать эти факторы.

Структура и основные параметры оптоволоконного кабеля подробно представлены в [28]. Волоконно-оптические кабели дифференцируются по размеру несущего волокна и оболочки – слоя стекла, отражающего свет. Кроме. того, различают ОКС по режиму передачи: одномодовые и многомодовые кабели, а также по используемой длине волны (850–1550 нс) и применяемым источникам света (лазеры или светодиоды – LED).

Основным элементом оптоволоконного кабеля является внутренний сердечник из стекла или пластика (рис. 4.6, позиция 1). Диаметр и прозрачность стекловолокна определяют количество передаваемого им света.

Наиболее распространены следующие типы оптоволоконного кабеля:

- с сердечником 8,3 мк и оболочкой 125 мк;
- с сердечником 62,5 мк и оболочкой 125 мк;
- с сердечником 50 мк и оболочкой 125 мк;
- с сердечником 100 мк и оболочкой 145 мк.

Волоконно-оптические кабели толщиной в 8,3 микрона очень трудно соединить точно. Поэтому возможны монтажные ошибки, в том числе и трудно выявляемые при тестировании кабельной линии. Подобные дефекты можно устранить установкой дополнительных оптоволоконных повторителей (концентраторов), увеличивающих уровень электромагнитных излучений кабельной системы в целом. Однако в последнее время на рынке появились так называемые заказные кабельные комплекты, то есть кабели с уже смонтированными и проверенными в заводских условиях коннекторами, исключающими процедуры монтажа и тестирования линии в полевых условиях.

Для оптоволоконного кабеля характерны следующие особенности:

- наличие центрального силового элемента;
- размещение в полимерной трубке-модуле;
- количество оптических волокон в одном модуле – от 1 до 12;
- заполнение пространства между модулями упрочняющими элементами – корделями из стеклонитей или нитей из кевлара и гидрофобным гелем;
- покрытие всех этих элементов и модулей промежуточной полимерной оболочкой;
- внешняя защита оболочки из полиэтилена или металла (возможно наличие двух защитных оболочек – металлической и полиэтиленовой).

Наряду с указанными общими особенностями оптоволоконные кабели различных фирм могут иметь дополнительные скрепляющие ленты, антикоррозийные и водозащитные обмотки, гофрированные металлические оболочки и т.д.

Как отмечалось выше, эффективным способом перехвата информации с оптоволоконных кабельных систем является непосредственное подключение к ним. Появилась информация о создании специальных дистанционно управляемых роботов, которые могут самостоятельно передвигаться по кабельным канализациям и подключаться к оптоволоконному кабелю для последующей передачи данных, циркулирующих в ОКС.

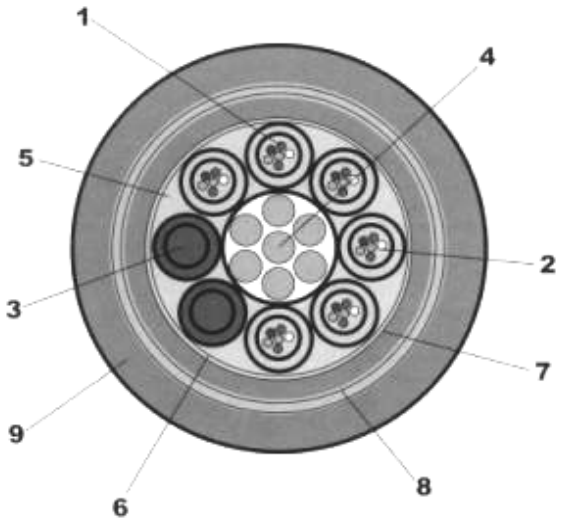


Рис. 4.6. Конфигурация оптоволоконного кабеля (на примере оптического городского кабеля производства фирмы Fujikara для прокладки в кабельной канализации, трубах, блоках, коллекторах, на мостах и в кабельных шахтах): 1 – оптическое волокно; 2 – внутримодульный гидрофобный заполнитель; 3 – кордель; 4 – центральный силовой элемент – стальной трос; 5 – гидрофобный заполнитель; 6 – скрепляющая лента; 7 –промежуточная оболочка из полиэтилена; 8 – броня из стальной гофрированной ленты; 9 – защитная оболочка из полиэтилена

Для противодействия злоумышленникам, имеющим специальную технику, было предложено использовать внутренние силовые металлические конструкции оптоволоконных кабелей в качестве сигнальных проводов. В этом случае невозможен доступ к оптоволокну без нарушения целостности силовых конструкций. Нарушение целостности приведет к срабатыванию сигнализации в центре контроля за ОКС. Дополнительного оборудования для реализации подобной охранной системы практически не требуется.

Параметры ОКС косвенно влияют на безопасность системы передачи данных в целом. Существуют одномодовый и многомодовый режимы передачи данных. По одномодовым волокнам передаются оптические сигналы с одной длиной волны. В многомодовых волокнах могут передаваться сигналы с различной длиной волны. Для совмещения нескольких оптических сигналов применяется так называемый волновой мультиплексор (Wave Division Multiplexer – WDM). WDM работает как призма. Сигналы с различной длиной волны комбинируются в нем, а затем пересылаются по одному из оптических волокон. Призма на приемном конце разлагает сигнал на волны исходной длины и направляет их на вход соответствующего оптического приемника. Применение мультиплексирования позволяет увеличить число возможных каналов передачи данных. Однако в многомодовых кабелях сигналы затухают сильнее, следовательно, расстояния между

узлами регенерации должны быть значительно уменьшены, что делает систему более дорогой, более «излучающей» и менее защищенной.

В целом же затухание сигналов в оптоволоконном кабеле (до 5 дБ/км) немного меньше затухания электрического коаксиального кабеля. Это объясняется тем, что свет не излучается вне кабеля, как электрический сигнал в медных проводах. Очень важно и то, что с ростом частоты более 200 МГц оптоволоконные кабели имеют несомненное преимущество перед любыми электрическими кабелями. Поэтому для обеспечения безопасности информации целесообразна высокочастотная передача.

Затухание сигнала существенно увеличивается при разветвлении и ответвлении кабеля. В связи с этим предпочтительнее использовать однонаправленные кабели, что, в свою очередь, определяет предпочтительные топологии сети: «звезда» (с двумя разнонаправленными кабелями между центральным абонентом и каждым из периферийных) или кольцо (с одним однонаправленным кабелем).

Несмотря на малое затухание, волоконной оптике присуща другая проблема – хроматическая дисперсия. Волны света различной длины стекло пропускает по-разному, поэтому импульс света, проходя через кабель, «размывается». Получается эффект радуги – световой сигнал разделяется на цветовые компоненты. На расстоянии в несколько километров он может «залезть» в следующий бит, что приведет к потерям данных. Это нарушит их целостность, которая является наряду с конфиденциальностью и доступностью важнейшим аспектом информационной безопасности. В одномодовых кабелях передается свет одной частоты, поэтому здесь нет эффекта хроматической дисперсии.

Одно из возможных решений указанной проблемы – увеличение расстояния между соседними сигналами и соответственно сокращение скорости передачи, что не всегда допустимо. Однако исследования показали, что при генерации сигнала в некоторой специальной форме дисперсионные эффекты почти исчезают, и сигнал можно передавать на тысячи километров. Сигналы в этой специальной форме называются силитонами.

К недостаткам оптоволоконного кабеля относятся меньшие механическая прочность и долговечность по сравнению с электрическим кабелем и снижение чувствительности при воздействии ионизирующих излучений.

Как было отмечено выше, компьютерные сети, построенные на базе оптоволоконных каналов, излучают в окружающее пространство конфиденциальные данные. Компания ITT Cannon NS&S провела ряд измерений уровня собственных излучений для оптоволоконной, экранированной и неэкранированной кабельных систем в специально оборудованных лабораториях. В результате оказалось, что на частотах до 70 МГц сеть на основе экранированной кабельной системы имеет самый низкий уровень собственных излучений. Это объясняется тем, что при хорошем заземле-

нии экранирование не только снижает на несколько порядков собственные излучения кабелей, но и уменьшает электрический потенциал корпусов активных устройств. На частотах 70–100 МГц все системы показали скачкообразные кривые амплитудно-частотных характеристик уровня собственных излучений, хотя характер их у всех систем был примерно одинаковым [23]. Появление пиков свидетельствует об образовании сложных колебательных контуров как в кабелях, так и в активном оборудовании.

Приведем пример влияния различных типов линий связи на вычислительную систему. При тестировании локальная вычислительная сеть функционировала в режиме передачи АТМ со скоростью 155 Мбит/с на линиях с незащищенной, с защищенной витой парой и с оптоволокном. В качестве воздействия рассматривалось радиочастотное поле с интенсивностью 3 В/м. Система на базе незащищенной витой пары характеризовалась высоким уровнем появления сбоев и в итоге вышла из строя. Локальная вычислительная сеть на оптоволокне имела сбои, но работала. И только локальная вычислительная сеть на основе защищенной витой пары была совершенно не подвержена помехам.

Таким образом, безопасность ОКС определяется самым «узким» местом телекоммуникационных систем – сетевым активным оборудованием.

Возможные каналы утечки информации в радиочастотном диапазоне известны и хорошо изучены. С начала 80-х годов велись работы по выявлению возможных каналов утечки информации в оптическом диапазоне частот. Для анализа возможных каналов утечки информации рассмотрим простейшую модель ВОСПИ согласно [23] (рис. 4.7).

В качестве излучателя для ВОСПИ могут использоваться полупроводниковые устройства двух типов. Устройство простейшего типа – светоизлучающий диод имеет широкую диаграмму направленности излучения и поэтому пригоден для работы с многомодовыми волоконными световодами с большим диаметром сердцевины. Более сложные устройства – полупроводниковые лазеры излучают значительно лучше сколимированные пучки света и поэтому позволяют вводить сигнал более высокой мощности (в 10–100 раз) в многомодовые световоды, а также эффективно вводить сигнал в одномодовые световоды с малым диаметром сердцевины. Светоизлучающие диоды вполне подходят для применения в информационных каналах и в системах связи с невысокой или умеренной пропускной способностью.

Утечка информации у излучателя возможна:

- за счет несоответствия геометрических размеров окна (микролинзы) светоизлучающего диода или полупроводникового лазера и торца (апертуры) волоконного световода;
- за счет «окон прозрачности» вокруг контактов на подложке, к которым подводится передаваемый информационный сигнал в радиочастотном диапазоне.

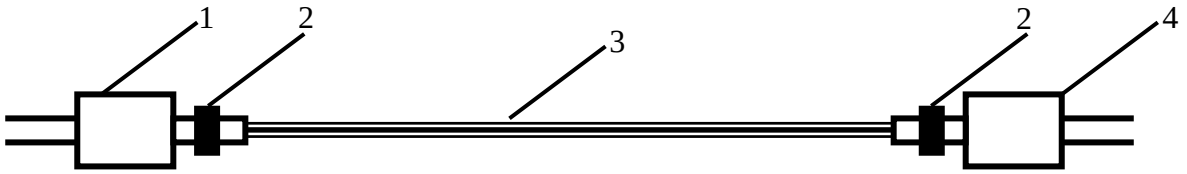


Рис. 4.7. Модель ВОСПИ: 1 – излучатель; 2 – оптический разъем; 3 – оптическое волокно; 4 – приемник

В качестве приемника в ВОСПИ, как правило, используются фотодиоды.

Утечка у приемника в оптическом диапазоне частот возможна:

- за счет несогласования геометрических размеров окна (микролинзы) фотодиода и торца волоконного световода;
- за счет «окон прозрачности» вокруг контактов на подложке, к которым подводится принимаемый информационный сигнал в радиочастотном диапазоне.

Для исключения утечки информации в оптическом диапазоне частот у излучателя и приемника необходимо, чтобы их конструкция с физической точки зрения представляла абсолютно «черное тело». Как правило, потери в оптических разъемах составляют 2,5–4,5 дБ.

Наибольший интерес представляет излучение информации с оптического волокна.

Абсолютно все волоконные световоды обладают затуханием. Затухание света в волоконном световоде обусловлено поглощением и рассеянием в материале, рассеянием, связанным со световодной структурой и потерями на излучение. Рассеяние, связанное со световодной структурой, вызвано большей частью геометрическими неоднородностями поверхности раздела сердцевина-оболочка. Тщательно контролируя процесс изготовления, можно поддерживать уровень потерь на рассеяние этого типа ниже 1 дБ/км. Потери на излучение вызваны изгибами световода и при малых радиусах кривизны могут быть значительными.

Излучение из волоконного световода достигает особенно больших величин, если при изготовлении оптического кабеля используются световоды без мягкой амортизирующей пластиковой оболочки.

С точки зрения утечки информации наиболее опасными являются «оболочечные» и «вытекающие» моды, так как, имея доступ к данному типу оптического волокна, с помощью высокочувствительных фотоприемных устройств (в качестве оптического объектива можно использовать микролинзы или специальное оптическое волокно, оптически согласованное с основным с помощью специально подобранной эмиссионной жидкости), можно принять передаваемый оптический сигнал.

Если в оптическом кабеле существуют нарушения структуры, напряжения, приложенные перпендикулярно оси оптического волокна, то они

могут вызывать его изгибы с малым радиусом кривизны. Осевые напряжения могут также приводить к изгибам, если имеются неоднородности структуры, к удлинению световода и росту микротрещин. Напряжение на выпуклостях может привести к изгибу световода и увеличению побочного излучения. Натяжение может также привести к увеличению микротрещин и вызвать изменение показателя преломления, что, в свою очередь, также может вызвать увеличение побочного излучения с волокна.

Частота f_0, при которой в диапазоне $f >= f_0$ имеет место излучение поля в окружающее пространство, называется частотой отсечки. Чем дальше от нее частота f, тем быстрее «высвечивается» энергия из волокна.

Все вышесказанное рассматривалось относительно волоконного световода. Если рассматривать оптический кабель, состоящий из нескольких оптических волокон, по которым передается конфиденциальная информация с разным грифом, то возникает еще один канал утечки информации за счет переходного затухания, обусловленного вытекающими модами.

При построении ВОСПИ для передачи конфиденциальной информации необходимо детально проанализировать условия эксплуатации, гриф информации, выбрать тип оптического кабеля, позволяющий осуществить защиту информации от возможной утечки за счет побочного излучения в оптическом диапазоне частот. Помимо конструктивных средств защиты информации можно использовать и активную защиту, в частности зашумление в оптическом диапазоне и квантовую криптографию.

4.4. Заземление технических средств и подавление информационных сигналов в цепях заземления

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 [6].

На рис. 4.8. показана наиболее простая последовательная одноточечная схема заземления, применяемая на низких частотах. 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 (рис. 4.9) этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления участков заземления. Применяется на низких частотах.

Многоточечная схема заземления (рис. 4.10) свободна от выше указанных недостатков, но требует принятия мер для исключения замкнутых контуров. Применяется на высоких частотах.

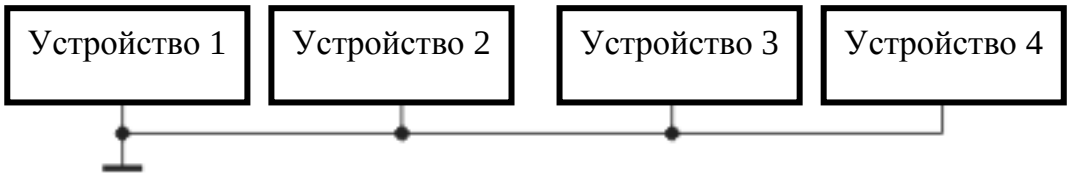


Рис. 4.8. Одноточечная последовательная схема

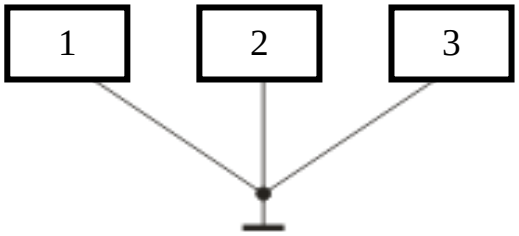


Рис. 4.9. Одноточечная параллельная схема

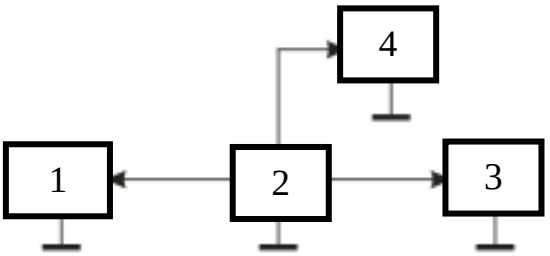


Рис. 4.10. Многоточечная схема

Комбинированные схемы представляют собой сочетание названных:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивление заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземленный элемент должен быть присоединен к заземлителю при помощи отдельного ответвления;
- в системе заземления должны отсутствовать замкнутые контуры;
- следует избегать использования общих проводников в системе экранируемых заземлений, защитных заземений и сигнальных цепей;
- минимальное сопротивление контактов (лучше пайка);
- контактные соединения должны исключать возможность образования оксидных пленок, вызывающих нелинейные явления;
- контактные соединения должны исключать возможность образования гальванических пар, вызывающих коррозию;
- запрещается использовать в качестве заземлителей нулевые фазы, металлические оболочки подземных кабелей, металлические трубы водо- и теплоснабжения.

Сопротивления заземления определяются качеством грунта. Орошение почвы вокруг заземления 5%-м соляным раствором снижает сопротивление в 5–10 раз.

Для эффективного подавления информативных сигналов в цепях заземления и электропитания применяют электрическое зашумление от генераторов шума.

4.5. Фильтрация информационных сигналов

4.5.1. Основные сведения о помехоподавляющих фильтрах

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 пределами устройства – источника опасного сигнала.

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры [6, 24].

Разделительные трансформаторы должны обеспечивать разводку первичной и вторичной цепей по сигналам наводки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения этих связей часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка первичной обмотки замыкается на землю. Однако электромагнитное поле вокруг экрана также может служить причиной наводки.

Разделительные трансформаторы решают задачи:

- разделение по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же цепям переменного тока;
- устранение ассиметричных наводок;
- ослабление симметричных наводок на вторичную обмотку.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивают ослабление информационного сигнала наводки на 126 дБ.

Помехоподавляющие фильтры обеспечивают ослабление нелинейных сигналов в разных участках частотного диапазона. Основное значение фильтров – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе, и подавлять сигналы за пределами полосы.

Количественная величина ослабления фильтра определяется ЛАЧХ

$$A = 20\lg\left(\frac{U_1}{U_2}\right) \qquad (4.14)$$

где U_1 – напряжение опасного сигнала на входе фильтра, U_2 – напряжение опасного сигнала на выходе фильтра.

Важнейшим условием защиты информации в технических средствах является создание специализированной базы технологических компонентов – помехоподавляющих изделий, необходимых для принятия схемотехнических мер по минимизации паразитных генераций и побочных излучений на этапе разработки любого электронного устройства.

Побочные излучения обусловлены тем, что в генераторных, усилительных и других функциональных каскадах электронных устройств могут возникать паразитные генерации и наводки. Если при разработке аппаратуры не принять мер подавления указанных процессов непосредственно в местах их возникновения, создаются условия для устойчивого генерирования, усиления и возникновения побочных излучений, уровень которых может превышать нормы допустимых радиопомех.

Излучения от устройств электронно-вычислительной техники модулированы полезным сигналом, существуют в виде полезных гармоник в широком диапазоне частот, распространяются как кондуктивно, так и в виде излучаемых электромагнитных помех и несут в себе сигнал с тем же информационным содержанием, что и обрабатываемые сигналы. Такие излучения могут быть приняты и выведены на экран монитора аппаратуры перехвата. Устройства средств вычислительной техники могут быть как источником, так и рецептором – устройством, восприимчивым к внешним электромагнитным помехам, и могут служить переизлучателем этих помех.

Побочные излучения и кондуктивные помехи создают каналы утечки информации, обрабатываемой в технических средствах.

Технические меры борьбы с электромагнитными помехами включают в себя меры подавления паразитных генераций – источников побочных излучений, экранирование аппаратуры от внешних электромагнитных полей и фильтрацию кондуктивных помех.

Фильтрация является основным и эффективным средством подавления (ослабления) кондуктивных помех в цепях электропитания, в сигнальных цепях интерфейса и на печатных платах, в проводах заземления. Помехоподавляющие фильтры позволяют снизить кондуктивные помехи, как от внешних, так и от внутренних источников помех.

Применение помехоподавляющих элементов позволяет оптимизировать схемотехнические и конструкторско-технологические решения с целью минимизации или полного устранения паразитных генераций и побочных излучений, снизить восприимчивость аппаратуры к внешним электромагнитным полям и импульсным сигналам, устранить возможные каналы утечки информации.

В соответствии с расположением полосы пропускания фильтра относительно полосы помехоподавления в частотном спектре различают четыре класса помехоподавляющих фильтров [24, 31], амплитудно-частотные характеристики которых показаны на рис. 4.11:

• фильтры нижних частот (низкочастотные) – ФНЧ, пропускающие сигналы в диапазоне частот от $\omega_1 = 0$ до ω_2 (рис. 4.11, *1*);

• фильтры верхних частот (высокочастотные) – ФВЧ, пропускающие сигналы в диапазоне частот от ω_1 до $\omega_2 = \infty$ (рис. 4.11, *2*);

• полосовые (полосно-пропускающие) – ПФ, пропускающие сигналы в диапазоне частот от ω_1 до ω_2 (рис. 4.11, *3*);

• заграждающие или режекторные (полосно-задерживающие) ЗФ, пропускающие сигналы в диапазоне частот от 0 до ω_1 и от ω_2 до ∞ (рис. 4.11, *4*)

В зависимости от типов элементов, из которых составлены фильтры, их делят на:

• реактивные, состоящие из элементов *L* и *C*;

• пьезоэлектрические, состоящие из кварцевых пластин;

• безындукционные пассивные, состоящие из элементов *r* и *C*.

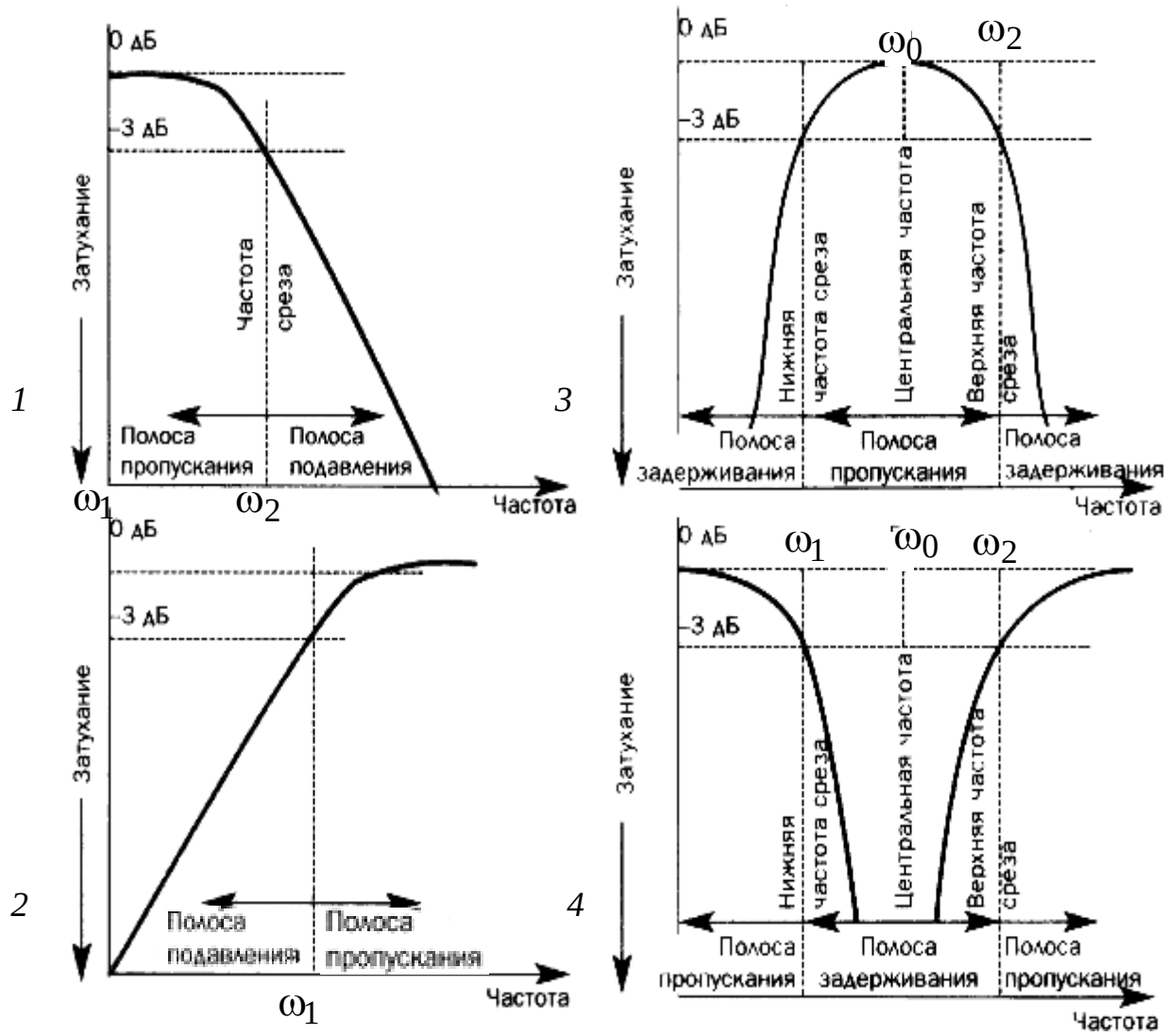


Рис. 4.11. Амплитудно-частотные характеристики помехоподавляющих фильтров: *1* – фильтра нижних частот, *2* – фильтра верхних частот, *3* – полосового фильтра, *4* – режекторного фильтра

Возможно применение активных *rC*-фильтров на основе микросхем (операционных усилителей). Это может быть целесообразно в тех случаях, когда пассивные *LC*-фильтры становятся очень громоздкими при понижении частоты среза до звуковых частот, когда даже при выборе относительно малой емкости (например, 0,01 мкФ) дроссель становится несоизмеримо большого размера и массы. В активном фильтре операционный усилитель преобразует импеданс подключаемой к нему *rC*-цепи так, что устройство ведет себя как индуктивность.

Для решения конкретных задач по обеспечению надежности функционирования, совместимости, помехозащищенности аппаратуры и других традиционных задач электромагнитной совместимости (ЭМС) чаще всего используются полосовые и режекторные фильтры.

Для целей обеспечения помехозащищенности информационных сигналов и защиты информации, обрабатываемой в технических средствах, от утечки по каналам побочных электромагнитных излучений и наводок, как правило, используются широкополосные *LC*-фильтры нижних частот.

Большинство высококачественных фильтров реализуются на основе катушек индуктивности и конденсаторов. *LC*-фильтры могут содержать также и резисторы. Связь входной и выходной цепей большинства фильтров соответственно с источником сигнала и нагрузкой производится таким образом, чтобы значения их реактивных или полных сопротивлений были равны нулю.

В большинстве *LC*-фильтров произведение полных сопротивлений емкости и индуктивности при изменении частоты остается примерно постоянным (из-за обратно пропорционального изменения их реактивных сопротивлений при изменении частоты). Например, если емкостное реактивное сопротивление снижается при увеличении частоты, то индуктивное реактивное сопротивление увеличивается на соответствующую величину. Такой фильтр называется *фильтром типа К*.

Ниже приводятся схемы некоторых типовых симметричных *LC*-фильтров.

На рис. 4.12 представлены симметричные Т-образный и П-образный *LC*-фильтры нижних частот. В Т-образном фильтре значения параметров выбираются по следующим выражениям:

$$L \approx \frac{2R}{\omega_2};\ \omega_2 \approx \frac{2}{\sqrt{LC}};\ C = \frac{2}{\omega_2 R}, \qquad (4.15)$$

где R или $Z \approx \sqrt{\frac{L}{C}}$ – активное или комплексное сопротивление нагрузки фильтра; $\omega_2 = 2\pi F_2$ – круговая частота среза фильтра (см. рис. 4.11); F_2 – линейная частота среза.

Формулы (4.15) могут быть выражены через линейную частоту среза:

$$L \approx \frac{R}{3{,}14F_2};\ F_2 \approx \frac{1}{3{,}14\sqrt{LC}};\ C \approx \frac{1}{3{,}14F_2R}. \qquad (4.16)$$

Суммарная индуктивность фильтра распределяется поровну между катушками (рис. 4.12, *а*).

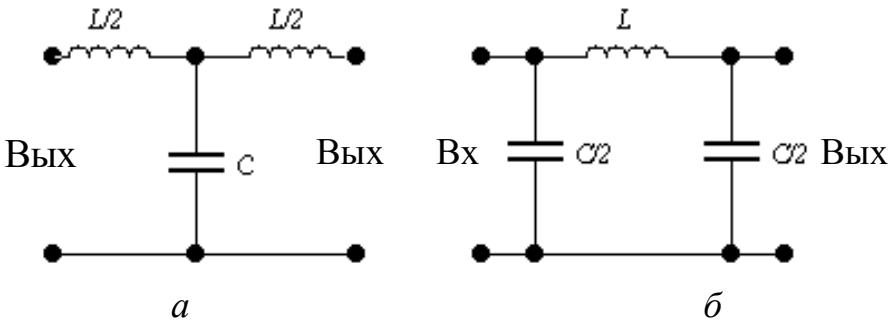


Рис. 4.12. Симметричные фильтры нижних частот:
а – Т-образный, *б* – П-образный

Для увеличения крутизны переходной области применяют П-образные фильтры (рис. 4.12, *б*). Требуемая общая емкость C распределяется поровну между конденсаторами фильтра. Расчет параметров фильтра проводится также по формулам (4.15) и (4.16).

На рис. 4.13 приведены схемы типовых *LC*-фильтров верхних частот Т-образной и П-образной структур. Фильтрам верхних частот также присуще то преимущество, что для переменного тока конденсаторы и катушки индуктивности работают противоположным образом. Следовательно, в *LC*-фильтров верхних частот последовательный элемент при увеличении частоты сигнала имеет более низкое реактивное сопротивление. Такой элемент пропускает высокочастотные сигналы, а для сигналов низких частот его реактивное сопротивление велико. Параллельный элемент оказывает шунтирующее влияние на сигналы низких частот, а для высокочастотных сигналов его реактивное сопротивление велико. Большинство *LC*-фильтров верхних частот являются фильтрами типа *K*.

Расчетные уравнения для Т-образного фильтра:

$$L \approx \frac{R}{2\omega_1};\ \omega_1 = 2\pi F_1;\ F_1 \approx \frac{1}{4\pi\sqrt{LC}};\ C \approx \frac{1}{4\omega_1 R}, \qquad (4.17)$$

где ω_1 – круговая частота среза (рис. 4.11, *2*), R или $Z \approx \sqrt{\frac{L}{C}}$ – активное или комплексное сопротивление нагрузки фильтра.

Требуемая суммарная емкость C распределяется поровну между конденсаторами фильтра так, что каждый конденсатор имеет емкость, равную удвоенному расчетному значению.

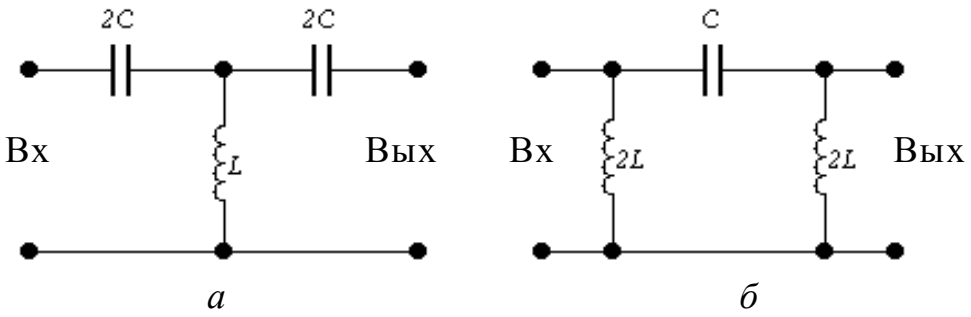


Рис. 4.13. Симметричные фильтры верхних частот:
а – Т-образный, *б* – П-образный

Для повышения крутизны частотной характеристики фильтра его выполняют по П-образной структуре (рис. 4.13, *б*). В фильтре требуемая общая индуктивность распределяется поровну между двумя катушками так, что каждая из них имеет индуктивность, равную удвоенному расчетному значению.

Расчетные формулы для определения параметров фильтра те же, что и для предыдущего случая.

На рис. 4.14 приведены схемы типовых полосно-заграждающих *LC*-фильтров Т-образной и П-образной структур. Полосно-заграждающий фильтр обладает тем преимуществом, что последовательные и параллельные резонансные цепи имеют различные характеристики их полных сопротивлений.

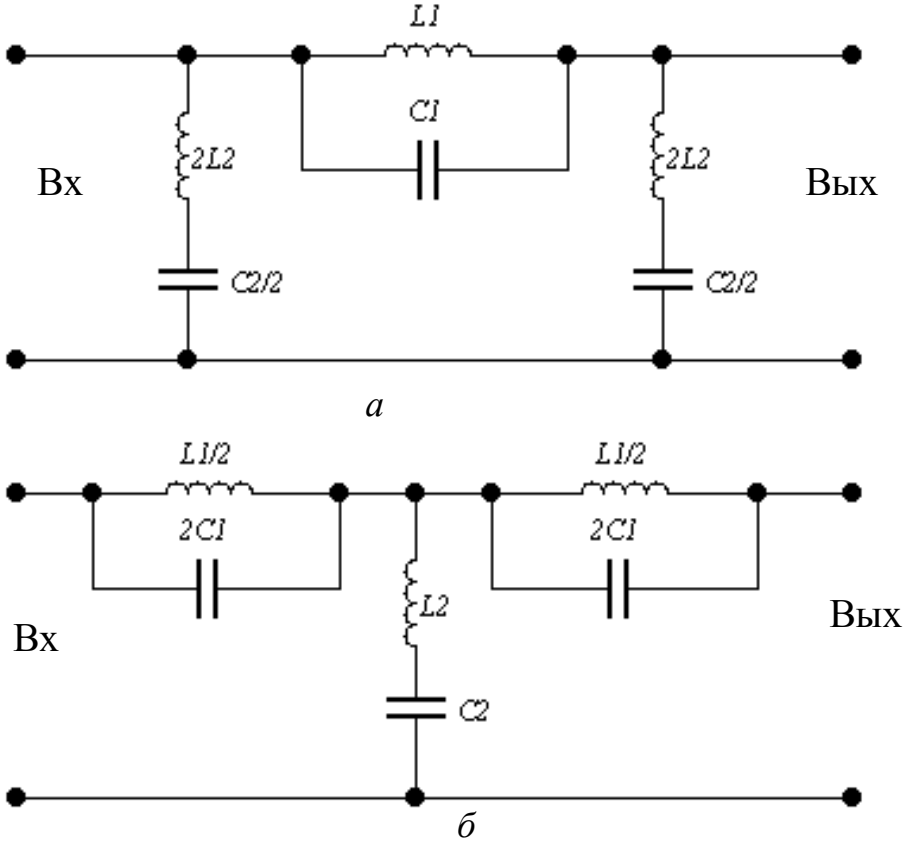


Рис. 4.14. Схемы полосно-заграждающих фильтров:
а – П-образнобразная; *б* – Т-образная

Параллельная *LC*-цепь создает на резонансной частоте максимально большое сопротивление в то время, как у последовательной цепи оно минимально. При соединении этих двух *LC*-цепей определенным образом, как показано на рис. 4.14, можно создать схему полоснозаграждающего фильтра. Последовательная ветвь обладает минимальным полным сопротивлением на центральной частоте требуемого диапазона. Ее полное сопротивление начинает увеличиваться по обе стороны от частоты резонанса. На центральной частоте эта ветвь оказывает шунтирующее воздействие. Параллельная ветвь на центральной частоте имеет максимальное сопротивление, и оно уменьшается по обе стороны резонанса. Эта ветвь препятствует прохождению сигналов в диапазоне частот по обе стороны от центральной частоты.

Для расчета параметров фильтров обеих структур можно воспользоваться следующими формулами:

$$L_1 \approx (\frac{\omega_2 - \omega_1}{2\pi}) \cdot \frac{4\pi R}{\omega_1 \omega_2}; \qquad L_2 \approx \frac{R}{2(\omega_2 - \omega_1)}; \tag{4.18}$$

$$C_1 \approx \frac{1}{2(\omega_2 - \omega_1)R}; \qquad C_2 \approx \frac{2(\omega_2 - \omega_1)}{R\omega_1\omega_2}; \tag{4.19}$$

$$F_{\text{рез}}(\text{кГц}) \approx \frac{159}{\sqrt{L(\text{мкГн})C(\text{мкФ})}}, \tag{4.20}$$

где $F_{\text{рез}}$ – частота резонанса.

На рис. 4.15 приведены схемы типовых полосно-пропускающих *LC*-фильтров Т-образной и П-образной структур.

Полоснопропускающий фильтр обладает тем преимуществом, что последовательные и параллельные резонансные цепи имеют различные характеристики их полных сопротивлений как и полоснозаграждающий фильтр. Параллельная *LC*-цепь создает на резонансной частоте максимально большое сопротивление в то время, как у последовательной цепи оно минимально. На основе этих двух *LC*-цепей можно реализовать полоснопропускающий фильтр. Последовательная ветвь обладает на центральной частоте требуемого диапазона минимальным полным сопротивлением, которое увеличивается по обе стороны от частоты резонанса. Эта ветвь оказывает шунтирующее воздействие на сигналы с частотами выше и ниже центра заданной полосы. Вследствие этого как последовательная, так и параллельная ветвь обеспечивают прохождение сигналов в диапазоне частот, лежащем по обе стороны от заданной центральной частоты.

Для расчета параметров фильтров обеих структур можно воспользоваться следующими формулами:

$$L_1 \approx \frac{2R}{\omega_2 - \omega_1}; \quad L_2 \approx \frac{(\omega_2 - \omega_1)R}{2\omega_1\omega_2}; \tag{4.21}$$

$$C_1 \approx \frac{\omega_2 - \omega_1}{2\omega_1\omega_2 R}; \quad C_2 \approx \frac{2}{(\omega_2 - \omega_1)R}; \tag{4.22}$$

$$F_{\text{рез}}(\text{кГц}) \approx \frac{159}{\sqrt{L(\text{мкГн})C(\text{мкФ})}}. \tag{4.23}$$

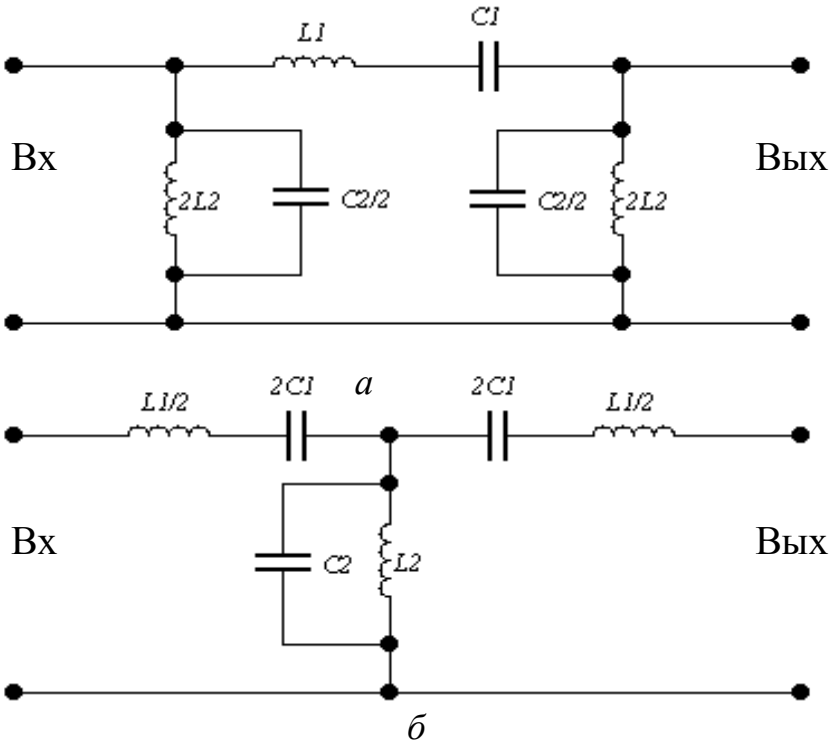


Рис. 4.15. Схемы полосно-пропускающих фильтров:
а – П-образнобразная; *б* – Т-образная

4.5.2. Выбор типа фильтра

Выбор необходимого типа фильтра зависит от электрической характеристики системы, в которую он должен быть установлен, требований по эффективности подавления помех, в том числе частоты среза и верхней предельной частоты ослабления, т.е. частотных характеристик фильтруемой цепи, а также требований, определенных условиями эксплуатации и от реальных ограничений по установке фильтра в аппаратуре. Все эти факторы увязываются с электрическими характеристиками фильтра.

Основные критерии выбора помехоподавляющего фильтра приведены в [24].

Помехоподавляющие фильтры выпускаются как зарубежными фирмами, так и предприятиями отечественной промышленности. Предприятиями электронной промышленности РФ выпускаются:

- сетевые помехоподавляющие фильтры корпусные;
- сигнальные проходные керамические помехоподавляющие фильтры;
- ферритовые помехоподавляющие изделия и элементы;
- электрические соединители, экранированные и с помехоподавляющими фильтрами-контактами.

Среди сетевых помехоподавляющих фильтров (СПФ), выпускаемых отечественной промышленностью, получили распространение фильтры, параметры которых приведены в табл. 4.1. Эти фильтры представляют собой *n*-звенные пассивные *LC*-фильтры, выполненные в герметичных металлических корпусах. Соединение входа-выхода фильтра с электросетью и нагрузкой осуществляется с помощью проходных контактов, состоящих из вывода, запрессованного в изолирующую втулку. Наружные металлические детали фильтра защищены от коррозии гальванопокрытием.

Таблица 4.1

Сетевые помехоподавляющие фильтры отечественного производства

№№ п/п	Наименование фильтра	Ток, А не более	Частотный диапазон, МГц	Вносимое затухание, дБ	Габаритные размеры, мм	Масса, кГ не более
1	ФПБМ-1/2/3	5/10/20	0,01...10000	60...90	240×75×55	1,8
2	ФТМА	0,5	0...4 0,01...1000	2 25...70	45×40×25	0,1
3	ФСГА	6	0,01...500	40...60	180×140×50	1,7
4	ФППС	3	0,1...1000	40...60	62×52×42	0,35
5	ФСБШ-2/4/7	1/2/5	0,01...500	15...50	104×90×60	0,6
6	ФСШК-1/2	3/6	0,1...1000	40...70	62×52×42	0,25
7	ФПБД	15	0,01...1000	30...60	104×94×52	0,6
8	ФСМА	30	0,01...1000	30...60	104×94×52	0,7
9	ФСБШ-9	10	0,01...1000	15...50	104×78×30	0,26

Почти все типы фильтров залиты эпоксидньм компаундом и рассчитаны на жесткие условия эксплуатации с гарантированным сроком не менее 5 лет со дня изготовления. В отличие от ранее разработанных фильтров (типов ФП, ФПВЧ, ФПС и др.) в этих фильтрах при синтезе их частотных характеристик были использованы паразитные параметры элементов и дроссели на составных магнитопроводах, что позволило значительно улучшить их удельно-объемные и удельно-весовые характеристики.

Среди отечественных сетевых помехоподавляющих фильтров в последнее время нашли широкое распространение пассивные *LC*-фильтры типа ФПБМ, ФСШК, ФСМА, которые соответствуют требованиям Гостех-

комиссии России по защите от утечки секретной информации за счет побочных электромагнитных излучений и наводок.

Некоторые образцы и их характеристики сетевых помехоподавляющих фильтров отечественного производства представлены на рис.4.16.

Фильтр сетевой для защиты от утечки информации от ПЭВМ и других средств передачи информации ФАЗА-1-10 (рис. 4.16) предназначен для предотвращения утечки информации от ПЭВМ и других технических средств передачи информации по линиям питающей сети, выходящими за пределы выделенного помещения или за границы контролируемой зоны, за счет подавления наводок опасных (информативных) сигналов.

Фильтр изготавливается в соответствии с требованиями по безопасности информации к аппаратуре военного назначения.

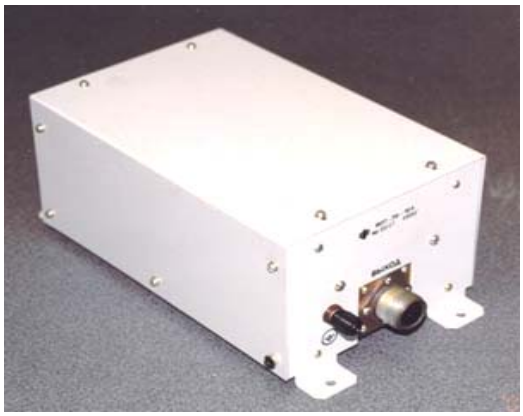


Рис. 4.16. Сетевые фильтры ФАЗА-1-10 и ФСП-3Ф-10А

ФСП-3Ф-10А представляет собой набор высокочастотных *LC*-фильтров, включаемых в сеть напряжением 220В частоты 50 Гц. Для уменьшения связи между входом и выходом *LC*-фильтры размещены в трех экранированных отсеках, образованных стенками и шасси фильтра. Соединение цепей между отсеками осуществляется проходными индуктивностями. Подавление помехи осуществляется реактивными *LC*-элементами фильтра.

4.6. Пространственное и линейное зашумление

Фильтрация относится к пассивным методам защиты. Когда фильтрация недостаточна по эффективности на границе контролируемой зоны, то прибегают к активным методам защиты, основанным на создании помех техническими средствами, что снижает отношение сигнал/шум.

Система пространственного зашумления должна обеспечивать [1]:

- электромагнитные помехи в диапазоне частот возможных побочных излучений ТСПИ;
- нерегулярную структуру помех;

- уровень создаваемых помех на электрический ток и по магнитной составляющей должен обеспечивать минимальное значение сигнал/шум;
- за счет выбора типа антенны помехи должны иметь горизонтальную и вертикальную поляризацию.

В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

«Синфазные помехи» с основном применяются для защиты ЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие по форме и времени существования с импульсами полезного сигнала. Вследствии этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, сигнал зашумления генерирует «имитационную помеху», по спектральному составу соответствующему спектральному сигналу.

Широкополосный сигнал помехи «белый шум» имеет равномерно распределенный энергетический спектр во всем рабочем диапазоне, существенно превышающий уровни побочных излучений. Такие системы применяются для защиты ЭВМ, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны.

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 (осветительной и розеточной сети).

Ниже приведены внешний вид и описание некоторых сетевых генераторов шума.

Генератор шума сетевой СОПЕРНИК (рис. 4.17) предназначен для обнаружения и подавления (в автоматическом режиме) устройств несанкционированного съема информации, использующих для передачи данных сеть 220 В.

Прибор предназначен для постоянной работы в дежурном режиме. СОПЕРНИК постоянно сканирует и анализирует сеть. При появлении в сети высокочастотной составляющей загорается красная светодиодная линейка, показывающая уровень сигнала, присутствующего в сети, и сразу же загорается зеленая светодиодная линейка, показывающая уровень шумового сигнала, генерируемого прибором в качестве противодействия. Автоматически включается вентилятор прибора, обеспечивающая нормальный

режим работы. При понижении в сети высокочастотного сигнала ниже определенного уровня прибор автоматически переходит в ждущий режим.

Прибор обеспечивает высокую эффективность защиты и не требует специальной технической подготовки пользователя.

Генератор шума SI-8001 (рис. 4.17) предназначен для защиты электросети переменного тока 220В / 50Гц от несанкционированного использования при передаче информации с помощью специальных технических средств. Принцип действия прибора основан на создании маскирующего сигнала (шума) в электросети в диапазоне частот от 5 кГц до 10 МГц. Генератор не оказывает влияния на работу персональных компьютеров и бытовой техники.

Рис. 4.17. Генераторы шума сетевые СОПЕРНИК и SI-8001

Генератор шума по сети электропитания IMPULSE (рис. 4.18) предназначен для блокирования каналов негласного съема информации из помещений по сети 220 В/50 Гц и линиям заземления. Позволяет нейтрализовать аппаратуру, использующую сеть электропитания в качестве канала передачи информации.

Рис. 4.18. Генераторы шума сетевые IMPULSE и NG-401

Свипирующий генератор белого шума сетевой NG-401 (рис. 4.18) предназначен для защиты электросетей переменного тока 220 В, 50 Гц от

несанкционированного их использования для передачи речевой информации. Принцип действия основан на подаче в защищаемую сеть сложного шумоподобного сигнала с цифровым формированием. Модификация изделия «NG-402» позволяет защищать одновременно три фазы силовой линии.

4.7. Способы предотвращения утечки информации через ПЭМИН ПК

В качестве технических способов исключения возможностей перехвата информации за счет ПЭМИН ПК можно перечислить следующие:

- доработка устройств ВТ с целью минимизации уровня излучений;
- электромагнитная экранировка помещений, в которых расположена вычислительная техника;
- активная радиотехническая маскировка (зашумление).

Доработка устройств ВТ осуществляется организациями, имеющими лицензии Гостехкомиссии России. Используя различные радиопоглощающие материалы и схемотехнические решения удается существенно снизить уровень излучений ВТ. Стоимость подобной доработки зависит от размера требуемой зоны безопасности и колеблется в пределах 20–70% от стоимости ПК. Электромагнитная экранировка помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат и не всегда возможна по эстетическим и эргономическим соображениям. Активная радиотехническая маскировка предполагает формирование и излучение в непосредственной близости от ВТ маскирующего сигнала.

Различают энергетический и неэнергетический методы активной маскировки. При энергетической маскировке с помощью генераторов шума излучается широкополосный шумовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучений ПК. Одновременно происходит наводка шумовых колебаний в отходящие цепи.

Из устройств активной энергетической маскировки наиболее известны: «Гном», «Шатер», «ИнейТ», «Гамма». Их стоимость достигает 25–30% от стоимости ПК. При установке такого устройства необходимо убедиться в достаточности мер защиты, так как в его частотной характеристике возможны провалы. Для этого потребуется привлечение специалистов с соответствующей измерительной аппаратурой.

Статистические характеристики сформированных генератором маскирующих колебаний близки к характеристикам нормального белого шума.

Более дешевыми являются генераторы шума ГШ-1000 и ГШ-К-1000. Генератор шума ГШ-1000 выполнен в виде отдельного блока с питанием от сети 220 В (рис. 4.19) и предназначен для общей маскировки ПЭМИ персональных компьютеров, компьютерных сетей и комплексов на объектах

АСУ и электронно-вычислительной техники первой, второй и третьей категорий.

Ш-К-1000 изготавливается в виде отдельной платы (рис. 13), встраиваемой в свободный слот системного блока персонального компьютера, и питается напряжением 12 В от общей шины компьютера.

Диапазон рабочих частот генераторов шума 0,01–1000 МГц. Спектральные характеристики обеих рассматриваемых моделей идентичны.

Возможности энергетической активной маскировки могут быть реализованы только в случае, если уровень излучений ПК существенно меньше норм на допускаемые радиопомехи от средств ВТ. В противном случае устройство активной энергетической маскировки будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемого средства ВТ, и потребуется согласование его установки со службой радиоконтроля.

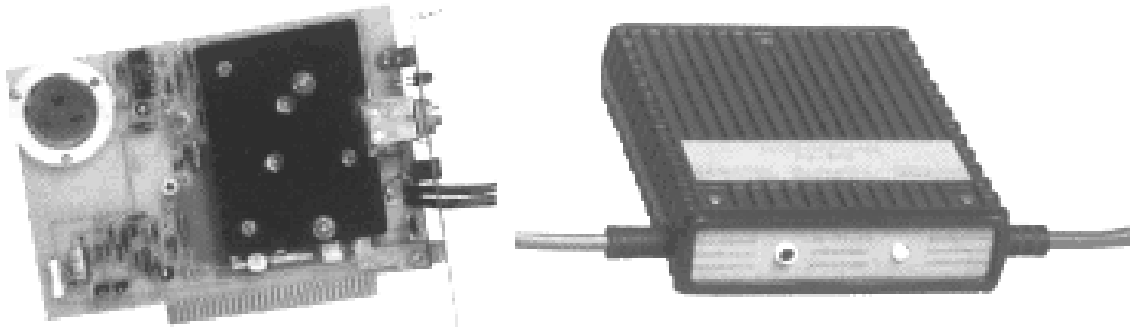


Рис. 4.19. Генераторы шума ГШ-К-1000 и ГШ-1000

Неэнергетический (статистический) метод активной маскировки заключается в изменении вероятностной структуры сигнала, принимаемого приемником злоумышленников, путем излучения специального маскирующего сигнала. Исходной предпосылкой в данном методе является случайный характер электромагнитных излучений ПК. Для описания этих излучений используется теория марковских случайных процессов. В качестве вероятностных характеристик применяются матрицы вероятностей переходов и вектор абсолютных вероятностей состояний. Сформированный с помощью оригинального алгоритма сигнал излучается в пространство компактным устройством, которое может устанавливаться как на корпусе самого ПК, так и в непосредственной близости от него. Уровень излучаемого этим устройством маскирующего сигнала не превосходит уровня информативных электромагнитных излучений ПК, поэтому согласования установки маскирующего устройства со службой радиоконтроля не требуется. Более того, подобные устройства в отличие от устройств активной энергетической маскировки не создают ощутимых помех для других электронных приборов, находящихся рядом с ними, что также является их неоспоримым преимуществом.

Установка и включение устройств активной маскировки, реализующих статистический метод, могут быть произведены без каких-либо трудоемких монтажных работ. Устройство не требует квалифицированного обслуживания, его надежная работа гарантируется встроенной схемой контроля работоспособности.

Следует отметить, что в случаях: доработки устройств ВТ, электромагнитной экранировки помещений и активной энергетической маскировки – показателем защищенности является отношение сигнал/шум, обеспечиваемое на границе минимально допустимой зоны безопасности. Максимально допустимое отношение сигнал/шум рассчитывается в каждом конкретном случае по специальным методикам. При активной радиотехнической маскировке с использованием статистического метода в качестве показателя, характеризующего защищенность, применяется матрица вероятностей переходов. В случае идеальной защищенности эта матрица будет соответствовать матрице вероятностей переходов шумового сигнала, все элементы которой равны между собой.

Несмотря на то, что для большинства руководителей предпринимательских структур утечка конфиденциальной информации из используемой ВТ через ПЭМИН кажется маловероятной, такой канал перехвата информации все же существует, а это значит, что рано или поздно кто-то им все-таки воспользуется. Особую остроту эта проблема приобретает для коммерческих фирм, офисы которых занимают одну или несколько комнат в здании, где кроме них размещаются другие организации. Универсального, на все случаи жизни, способа защиты информации от перехвата через ПЭМИН ПК, конечно же, не существует. В каждом конкретном случае специалистами должно приниматься решение о применении того или иного способа защиты, а возможно и их комбинации. И все же для большинства малых и средних фирм оптимальным способом защиты информации с точки зрения цены, эффективности защиты и простоты реализации представляется активная радиотехническая маскировка.

4.8. Устройства контроля и защиты слаботочных линий и сети

4.8.1. Особенности слаботочных линий и сетей как каналов утечки информации

При решении задачи обеспечения безопасности помещения необходимо учитывать, что злоумышленник может использовать телефонные и электросиловые линии, проходящие в здании, следующим образом.

Электросиловые линии используются для подслушивания разговоров в помещениях, через которые проходит линия. Как правило, линия используется в качестве источника питания подслушивающих устройств, пере-

дающих информацию из помещения по радиоканалу. Линия может использоваться и в качестве проводного канала. Достоинство такого канала передачи является большая, чем у радиоканала, скрытность, недостатком – что приемник информации необходимо подключать к той же линии, причем не дальше первой трансформаторной подстанции.

При использовании электросиловой линии в качестве источника питания подслушивающее устройство может быть подключено параллельно или последовательно линии. Параллельное подключение более предпочтительно, так как при нем подслушивающие устройство для питания использует напряжение линии и может работать практически в любое время (напряжение к линии приложено практически постоянно).

Для увеличения скрытности устройства при таком подключении могут применяться так называемые «сторожевые устройства», отключающиеся от сетевых проводов на несколько часов при кратковременном пропадании сетевого напряжения в линии. Последовательное подключение менее удобно для работы подслушивающего устройства, так как в этом случае для питания используется ток линии, а он появляется в линии только при подключении нагрузки.

Телефонные линии используются:

- для подслушивания телефонных разговоров (линия используется, как источник информационного сигнала, и может при этом использоваться как источник питания);
- для подслушивания разговоров в помещениях, вблизи которых проходит телефонная линия (телефонная линия используется как скрытный канал передачи информации в любое место, где есть телефон, и как источник питания);
- в качестве бесплатного канала телефонной связи (междугородные переговоры за чужой счет) и для проникновения в банковскую компьютерную сеть для присвоения денег (в том случае, если используется телефонная линия для пересылки финансовых документов).

При подслушивании телефонных разговоров специальное радиоэлектронное устройство может быть подключено в любом доступном для злоумышленников месте (в телефонном аппарате; в помещениях, в которых проходит линия, в распределительных коробках и шкафах здания; в узловых распределительных шкафах городской телефонной сети; на АТС) и подключаться параллельно линии (гальванически) или последовательно (гальванически или индуктивно).

При подслушивании разговоров в помещении специальное радиоэлектронное устройство может быть подключено только в помещении, которое хотят прослушать, и включаться только параллельно линии (гальванически), а работать может только в то время, когда телефоном не пользуются.

В качестве канала телефонной связи, а также для проникновения в банковскую систему, специальное радиоэлектронное устройство может быть подключено в любом доступном для злоумышленников месте, устройство может включаться только параллельно линии (гальванически) и работать только в то время, когда телефонной линией не пользуются.

4.8.2. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании

В зависимости от типа анализатора, используемого для контроля на закладные устройства силовых и телефонных линий, рекомендуются типовые схемы обследования линий.

При применении анализатора линий КОМ-2М рекомендуются типовые схемы его подключения, показанные на рис. 4.20, 4.21, 4.22 и 4.23.

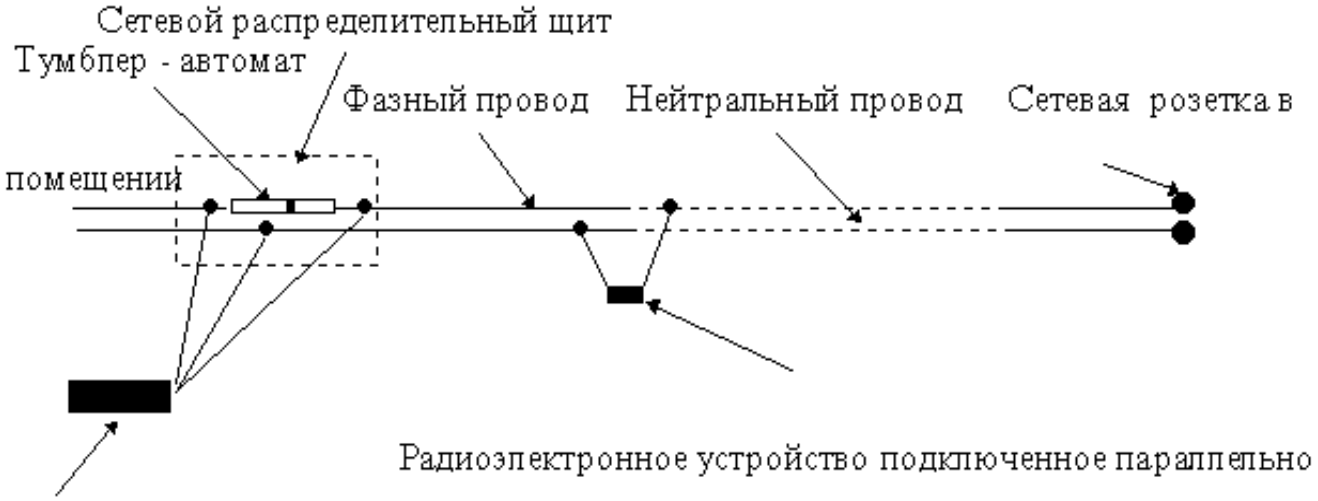


Рис. 4.20. Схема обследования электросиловой линии в режиме холостого хода

Анализатор линий КОМ-2М предназначен для обследования электросиловых и слаботочных линий (в том числе телефонных), с целью обнаружения микропотребляющих блоков питания, передатчиков и приемников подслушивающих устройств, негласно установленных на линиях.

Принцип действия анализатора основан на измерении и анализе следующих параметров линий:

- вольтамперной характеристики линии в режимах «холостого хода» (хх) и «короткого замыкания» (кз);
- импеданса линии в режиме «холостого хода»;
- тока утечки электросиловой линии на частоте 50 Гц;
- сопротивления изоляции линии на постоянном токе.

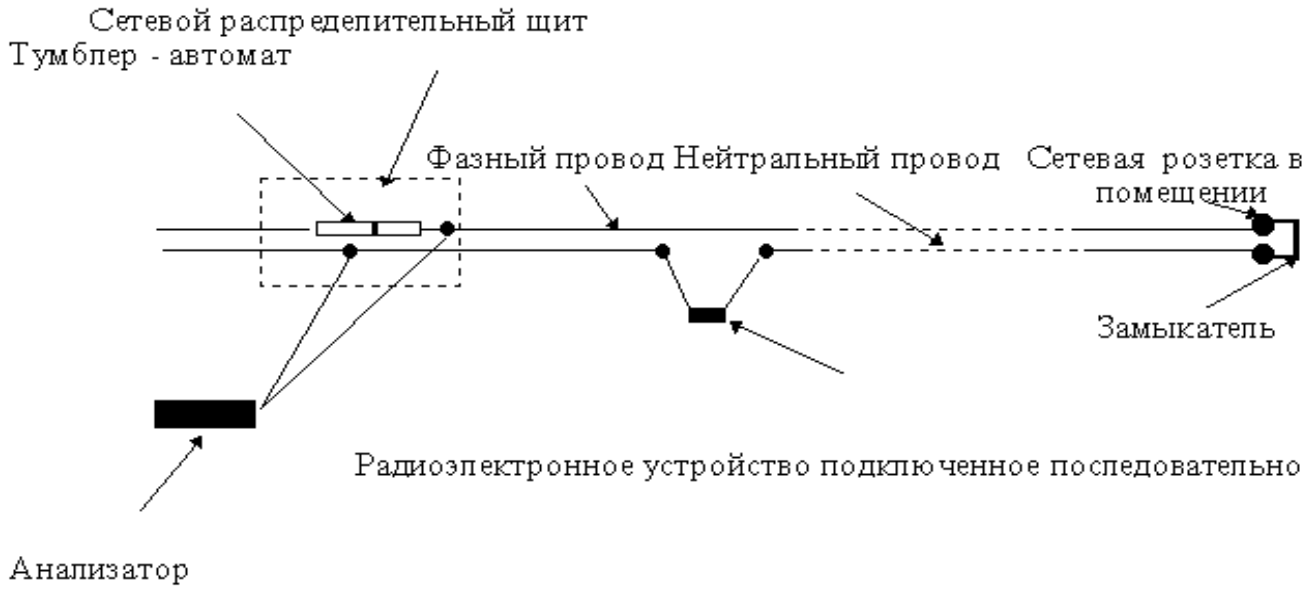


Рис. 4.21. Схема обследования электросиловой линии
в режиме короткого замыкания

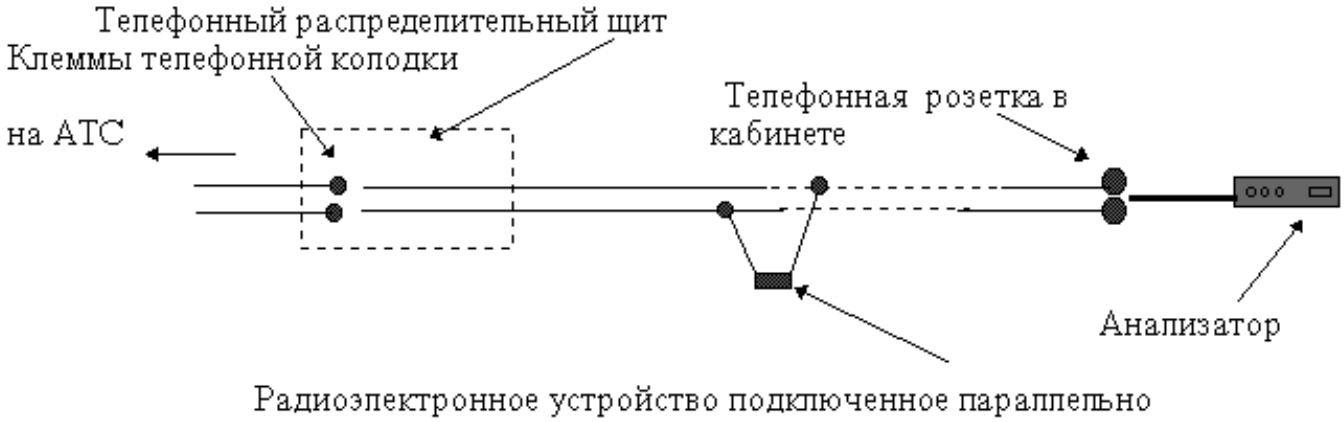


Рис. 4.22. Схема обследования телефонной линии в режиме холостого хода

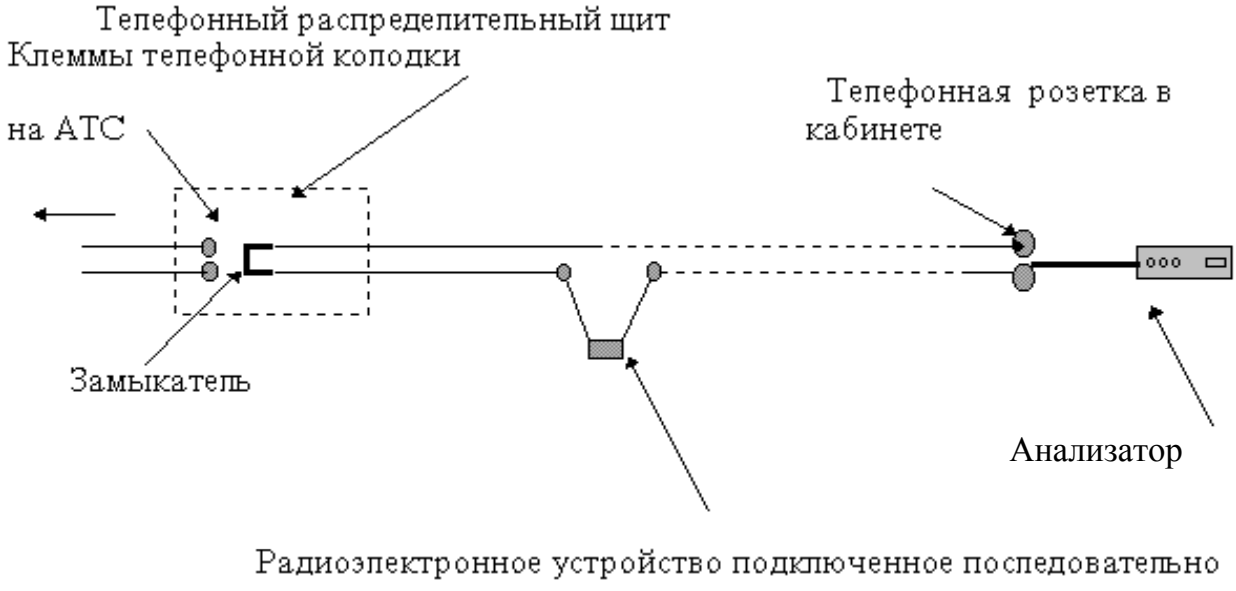


Рис. 4.23. Схема обследования телефонной линии
в режиме короткого замыкания

Вольтамперные характеристики линии анализируются так называемыми методами «нелинейной локации» с приемом второй и третьей гармонических составляющих испытательного напряжения.

Импеданс линии (точнее его отклонение от типовых значений) анализируется методом измерения переходных процессов импульсных сигналов в линиях.

Ток утечки и сопротивления изоляции измеряются стандартными методами, применяемыми в современных мультиметрах.

Определение прохождения обследуемой телефонной пары в телефонном распределительном шкафу производится путем подачи в линию специального тестового сигнала и фиксация его индуктивным датчиком приемника тестового сигнала в распределительном шкафу.

Анализатор характеризуется следующими техническими возможностями:

- позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных параллельно к линии, с мощностью потребления – 10 мкВт и более, оборудованных сторожевыми устройствами;
- позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных последовательно к электросиловой линии, с мощностью потребления – 100 мкВт и более;
- напряжение испытательного сигнала (220 ± 20)В на частоте 50 Гц;
- чувствительность на второй и третьей гармонике испытательного напряжения не хуже – 10 мкВ;
- анализатор позволяет фиксировать отклонения импеданса линии от типового значения, при подключении к линии последовательно соединенных конденсатора с емкостью 100 пФ и более и резистора с сопротивлением 1 МОм;
- диапазон измерения токов утечки от 0.1 до 200 мА;
- диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом;
- анализатор позволяет определять нахождение обследуемой телефонной пары в телефонных распределительных шкафах;
- длина обследуемых линий – до 100 метров;

питание от сети переменного тока напряжением 220 В частотой 50 Гц.

Для защиты информации от утечки по проводным линиям разработаны многочисленные устройства, часть из которых рассматривается ниже.

4.8.3. Устройства контроля и защиты проводных линий от утечки информации

Коммутатор-конвертер для поиска и анализ сигналов в сети 220 В и проводных линиях RS/KL (рис. 4.24) расширяет возможности комплексов обнаружения и локализации радиомикрофонов RS turbo M, построенных на

базе сканирующих радиоприемников. Он дает возможность сканеру принимать низкочастотные сигналы, которые передаются по проводам сети переменного тока с напряжением 220 В и по проводным, в частности, по телефонным линиям без модуляции или на несущих частотах от 600 Гц до 10 МГц. Входы коммутатора-конвертера 1,2,3 предназначены для анализа трёх фаз электропитания, входы 4, 5, 6, 7 – для анализа слаботочных линий.

Необходимый режим работы выбирается в настройках программы: конвертер RS/KL подключается как антенный коммутатор RS/K с адресом 4 с подключёнными к его входам конвертерами RS/L. Во время анализа приемник перестраивается в диапазоне частот 10 МГц вверх от частоты преобразования конвертера.

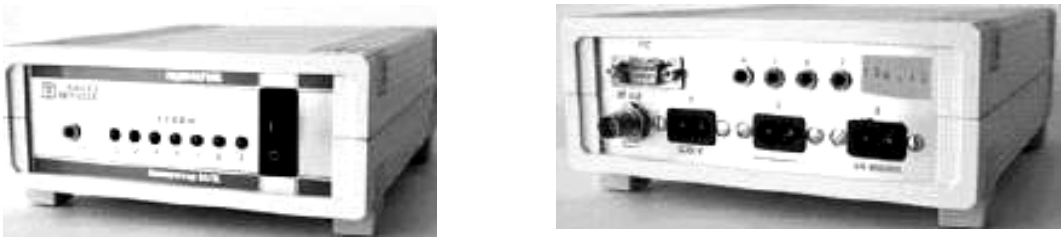


Рис. 4.24. Коммутатор-конвертер RS/KL

Программное обеспечение комплексов RS turbo M компании «Радиосервис» в режиме работы с конвертером автоматически пересчитывает и отображает на спектральных панорамах и в списках истинные частоты обнаруженных сигналов.

Изделие МП-3 (рис. 4.25) исключает утечку информации по цепи питания ТСПИ при акустическом воздействии на них и отключенном питающем напряжении [57].

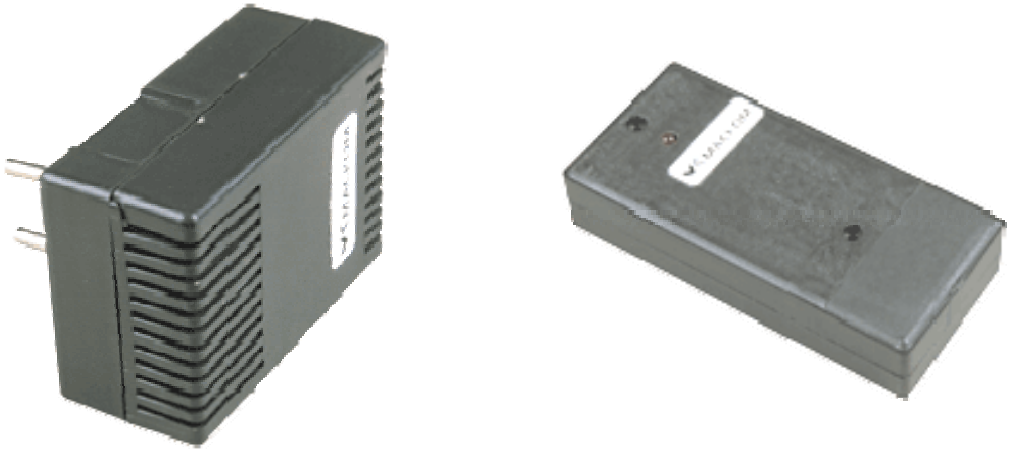


Рис. 4.25. Изделия для защиты линий МП-3 и МП-5

В отличие от других изделий, в которых обеспечивается необходимое затухание для информационного сигнала с помощью только какой-либо одной цепи, в «МП-3» реализуется одновременно как разрыв цепи питания

с помощью контактов реле, так и затухание с помощью диодно-емкостной цепи, что в сумме обеспечивает внесение затухания на частоте f = 1 кГц более 90 дБ.

Интервал регламентных работ определяется лишь вероятностью внештатного замыкания контактов реле. Все стальные неисправности являются обнаруживаемыми.

Изделие МП-5 (рис. 4.25) предназначено для защиты громкоговорителей системы оповещения или однопрограммных приемников от утечки через них акустических сигналов помещения [57]. При отсутствии сигналов оповещения (или сигналов трансляции) громкоговоритель отключен с помощью контактов реле. При появлении штатного сигнала через время t < 5 мс громкоговоритель включается и это состояние удерживается, если t паузы < 10 с. При этих параметрах изделие МП-5 не влияет на качество сообщения. При отключенном громкоговорителе акустоэлектрический сигнал, измеренный на частоте f = 1 кГц, до попадания в трансляционную линию претерпевает затухание < 90 дБ, чем обеспечивается исключение утечки информации из помещения по цепи трансляции.

Изделия МП-1А, МП-1Ц (рис. 4.26) включают в себя как активные средства защиты (АСЗ), так и пассивные средства защиты (ПСЗ) [57].

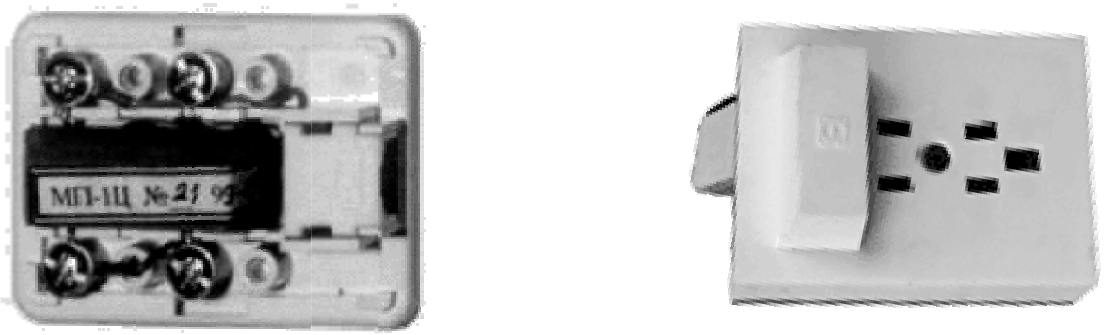


Рис. 4.26. МП-1А и МП-1Ц в российском корпусе и в евророзетке

Изделия МП-1А и МП-1Ц защищают информацию от утечки соответственно в аналоговых и цифровых ТА в режиме ожидания вызова. ПСЗ построены по принципу изделия «Гранит-8», а АСЗ – по принципу изделий «Гранит-11» и «Гранит-12».

Существенным в изделиях МП-1А и МП1-1Ц является то, что, превосходя по всем специальным параметрам указанные изделия типа «Гранит», они на порядок и более выигрывают в массогабаритных характеристиках и потребляемой мощности, что позволяет разместить их внутри телефонных розеток различных типов.

Устройство комплексной защиты телефонной линии ПРОТОН (рис. 4.27) обеспечивает:

• Визуальную и звуковую (отключаемую) индикацию при нарушении целостности телефонной линии (короткое замыкание, обрыв).

• Цифровую индикацию постоянной составляющей напряжения в телефонной линии во всех режимах работы (режим «АТЛ»).

• Работу встроенного вызывного устройства с пороговой регулировкой уровня звука (высокий/низкий).

• Развязку телефонного аппарата от телефонной линии при положенной трубке. Питание телефонного аппарата от отдельного стабилизированного внутреннего источника тока (исключает использование резонирующих свойств электромагнитных вызывных устройств).

• Шумовую помеху в звуковом диапазоне частот (отключаемую) в телефонную линию при положенной трубке (активизация диктофонов, препятствует прослушиванию помещения).

• Автоматическое включение режима минимального тока в телефонной линии без ухудшения качества связи после набора номера абонента.

• Обнаружение и противодействие попытке непосредственного прослушивания телефонной линии во время разговора (параллельный аппарат, низкоомные наушники и др.).

• Оперативное включение/выключение шумовой помехи, с автоматическим включением режима минимального тока в телефонной линии, в режиме «разговор».

Устройство активной защиты информации BFG (рис. 4.27) предназначено для активной защиты информации от перехвата средствами радиоэлектронного контроля.

Рис. 4.27. Устройство комплексной защиты телефонной линии «ПРОТОН» и устройство активной защиты информации BFG-01

Устройство представляет собой широкополосный генератор, который создает маскирующий сигнал, затрудняющий прием и расшифровку информации, содержащейся в электромагнитном излучении различных элек-

тронных приборов. Устройство имеет выходную мощность, достаточную для защиты информации от утечки не только за счет противодействия перехвату внешних электромагнитных полей средств оргтехники, но и за счет подавления излучений различного рода радиомикрофонов с мощностью излучения до 1 мВт, скрытно размещенных в охраняемом помещении или в непосредственной близости от него.

Прибор делает невозможной двустороннюю связь с помощью радиостанций и сотовых телефонов, существенно снижает вероятность срабатывания радиоуправляемых взрывателей в защищаемом объеме.

Стационарный генератор шума для радиотехнической маскировки и защиты цепей питания ГНОМ-3М (рис. 4.28) предназначен для защиты цепей первичного электропитания и радиотехнической маскировки рабочего помещения [64].

Рис. 4.28. Стационарные шумогенераторы ГНОМ-3М и ГНОМ-3

Система контроля функционирования генератора обеспечивает:

- индикацию наличия генерации (свечение светодиода «РАБОТА»);
- выдачу сигнала «АВАРИЯ» в виде уровня напряжения логического «0» на выходе, при этом светодиод «РАБОТА» гаснет.

Генератор шума ГНОМ-3М работает в диапазоне 150 КГц – 1000 МГц, имеет 4 корреляционно не связанных канала (выхода) для подключения к антенным контурам и цепям первичного электропитания, улучшенные весогабаритные характеристики.

Стационарный шумогенератор ГНОМ-3 (рис. 4.28) предназначен для защиты помещений и объектов электронно-вычислительной техники от утечки конфиденциальной информации за счет побочных электромагнитных излучений компьютеров и другой оргтехники. Работает в диапазоне частот шумового сигнала: 10 кГц ... 1 ГГц. Антенны – рамочные, монтируемые в 3-х плоскостях.

Генератор шума ГРОМ – 4 (рис. 4.29) предназначен для защиты от утечки информации за счет побочных электромагнитных излучений средств оргтехники, а также для создания помех устройствам несанкционированного съема информации с телефонных и электрических сетей.

Генератор обеспечивает:

- пространственное зашумление в диапазоне 20–1000 МГц, мощность 5 Вт;
- линейное зашумление электросети в диапазоне 0,1–1 МГц, мощность 4 Вт;
- использование эффекта «размывания» спектра акустического сигнала в телефонных линиях;
- независимую работу всех трех режимов.

Устройство защиты телефонных переговоров от прослушивания и записи ПРОКРУСТ ПТЗ-003 (рис. 4.29) предназначено для защиты телефонных переговоров от прослушивания. Подавитель обеспечивает защиту телефонной линии от различных типов телефонных подслушивающих устройств на участке от телефонного аппарата до АТС. Защита осуществляется путем изменения параметров стандартных сигналов. Изделие имеет цифровой дисплей – указатель напряжения на телефонной линии и световой индикатор снятия телефонной трубки.

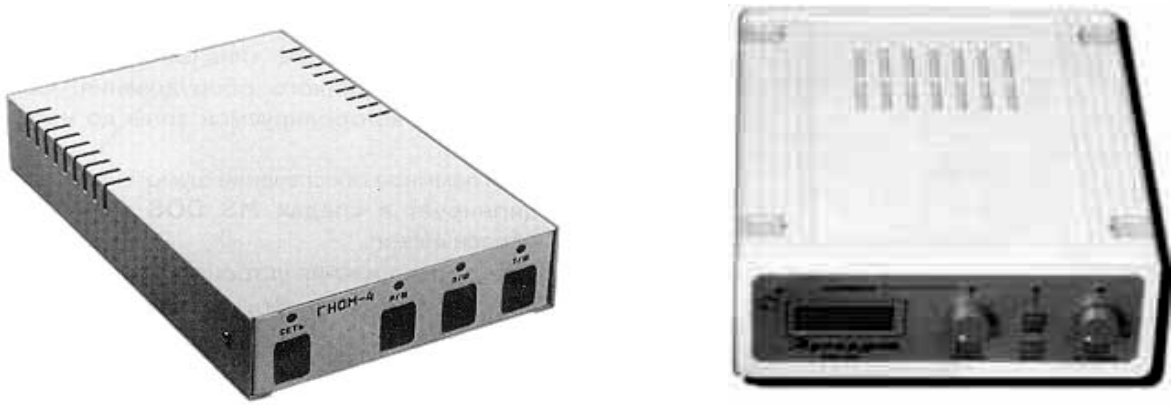


Рис. 4.29. Генератор шума ГРОМ-4
и устройство защиты телефонных переговоров ПРОКРУСТ ПТЗ-003

В подавителе предусмотрено три режима подавления, которые могут включаться независимо друг от друга, имеется возможность экстренного отключения всех режимов защиты, подключения диктофона для записи телефонных переговоров. Режим «Уровень» позволяет поднимать напряжение в телефонной линии во время разговора. В режиме «Шум» в линию подается шумовой сигнал звукового диапазона частот при положенной на рычаг телефонной трубке. В режиме «ВЧ помеха» в линию подается высокочастотный помеховый сигнал вне зависимости от положения телефонной трубки.

Прибор для защиты телефонных линий RPT-07 (рис. 4.30) предназначен для защиты переговоров по телефонной линии от несанкционированного съема информации. Прибор защищает одну телефонную линию на

участке «ТЛФ – аппарат – ГТС» как при поднятой, так и при положенной трубке телефонного аппарата.

Рис. 4.30. Приборы для защиты телефонных линий RPT-07 и Antifly

Прибор обеспечивает эффективное противодействие:

- радиопередатчикам, включенным в линию последовательно и параллельно (в том числе с бесконтактным съемом и внешним питанием);
- аппаратуре магнитной записи (в т.ч. цифровой), подключаемой к линии контактным или бесконтактным способом;
- параллельным ТА и аналогичной аппаратуре;
- аппаратуре, использующей «ВЧ-навязывание» и «микрофонный эффект»;
- аппаратуре, использующей линию в качестве канала передачи или в качестве источника электропитания.

Прибор имеет выход для подключения головных телефонов или диктофона.

Многофункциональное устройство защиты телефонной линии Antifly (рис. 4.30) предназначено для защиты телефонной линии от различных посторонних вмешательств. Устройство подключается между защищаемым телефонным аппаратом (группой аппаратов) и телефонной линией.

Оставаясь практически незаметным для защищаемого аппарата. устройство обеспечивает следующие защитные функции:

- *Контроль подключения при помощи «мухи»*. При подобном подключении в линии «проскакивают» специфические сигналы (1200 Гц или 2600 Гц). При приеме подобного сигнала устройство, в зависимости от настроек, либо выдает сигнал отбоя для «мухи», либо просто сообщает о попытке подключения при помощи звуковой или световой индикации.
- *«Подавление диктофонов»* – при положенной трубке устройство выдает в линию специальный сигнал, активизирующий (включающий) диктофоны, которые, возможно, подключены к вашей линии. В результате, вместо ваших разговоров диктофоны будут записывать этот сигнал, тратя на это свою пленку.

• *Блокировка незаконного набора*. При попытке подключения и набора номера с линии пользователя при помощи параллельной трубки, устройство включает индикацию и блокирует линию, делая набор невозможным. Под параллельным телефоном понимается любой аппарат, подключенный к линии между устройством и АТС.

• *Контроль параллельного подключения*. Если во время разговора будет снята трубка параллельного телефона, устройство сообщит об этом световой или звуковой индикацией. В устройстве предусмотрена возможность изменения следующих параметров: тип реакции на снятие параллельной трубки, тип реакции на подключение «мухи», чувствительность приемника (3 уровня). Так же имеется возможность регулировки чувствительности датчика параллельного подключения (датчика снятия трубки параллельного телефона). Наличие этих настроек позволяет оптимизировать работу устройства.

Дифференциальный адаптер проводных линий ДАПЛ 031 (рис. 4.31) обеспечивает:

• обнаружение устройств негласного съема информации, использующие для передачи информации проводные линии;

• оценку воздействия ПЭМИН.

Симметричный вход адаптера позволяет эффективно подавлять внешние помеховые сигналы.

Высокая чувствительность адаптера позволяет обнаруживать:

• передачу сигнала от микрофонов как активных так и пассивных (не имеющих предварительного усилителя).

• наличие «микрофонного эффекта» от средств оргтехники, бытовой РЭА, охранно-пожарной сигнализации и др. в исследуемой линии.

Конструкция измерительных щупов аналогична адаптеру проводных линий и позволяет подсоединять штатные насадки типа «Игла», «Сеть» и «Крокодил».

Рис. 4.31. Адаптер проводных линий ДАПЛ 031
и генератор высоковольтных импульсов RPT-02

Подавитель телефонных закладок RPT-02 (рис. 4.31) выполняет следующие функции:

- подавление последовательных и параллельных телефонных радиозакладок;
- отслеживание изменений нагруженности ТЛФ-линии, причиной которого может быть несанкционированное подключение;
- индикация и запоминание пропадания напряжения на линии, причиной которого может быть несанкционированное подключение;
- «выматывание» магнитной ленты диктофонов с акустическим пуском, поставленных на автоматическую запись.

Прибор предназначен для работы как с городской АТС, так и с мини-АТС.

Анализатор проводных коммуникаций LBD-50 (рис. 4.32) обеспечивает поиск гальванических подключений к проводным и кабельным линиям любого назначения. Обнаруживает несанкционированные устройства, подключенные к легальным коммуникациям для:

- перехвата информации;
- передачи материалов перехвата;
- обеспечения электропитанием.

Рис. 4.32. Анализатор проводных коммуникаций LBD-50

В анализаторе реализован комплекс методов обнаружения, как хорошо известных, так и оригинальных, не имеющих аналогов в мировой практике. Алгоритм обследования, заложенный в анализаторе, исключает срабатывание защитных сторожевых схем в объектах поиска.

4.9. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам

Если акустические и виброакустические характеристики защищаемого помещения не соответствуют нормативным требованиям по защите речевой информации, то применяют активные средства защиты. Они представляют собой генераторы акустического и виброакустического маскирующего шума, содержащие аудиоизлучатели, виброизлучатели и пьезоизлучатели.

Наиболее известными генераторами являются «СОНАТА – АВ 1М» и «ШОРОХ».

«СОНАТА – АВ 1М» (рис. 4.33) позволяет перекрыть большинство технических каналов утечки речевой информации, имеет сертификат соответствия требованиям безопасности информации выданный ГТК РФ, ги-

гиенический сертификат соответствия, имеет независимую регулировку уровня помех в каждом канале.

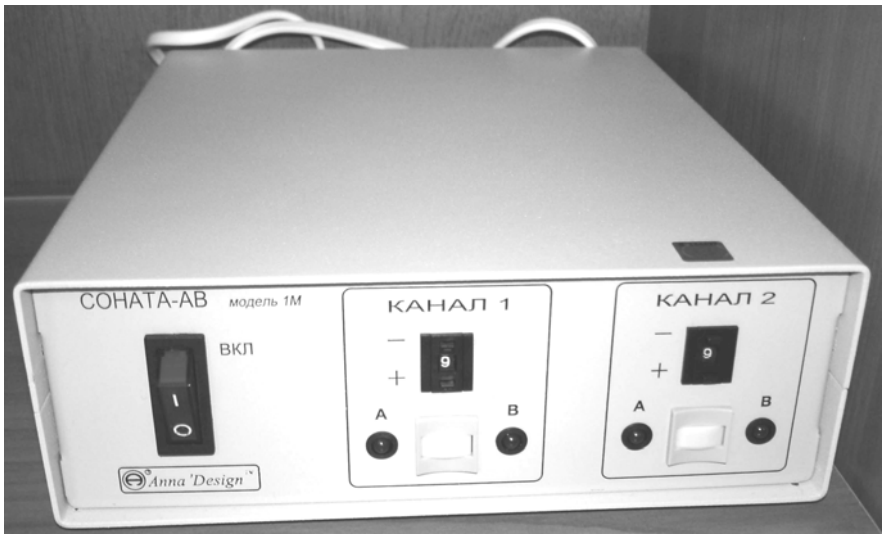


Рис. 4.33. Генераторный блок СВАЗ «Соната-АВ»

Стабильность основных характеристик генераторов «Соната-АВ» обеспечивается применением цифровых формирователей шума. Стойкость создаваемой генератором заградительной помехи к различным методам ее нейтрализации обеспечивается большим периодом используемых последовательностей и шумовой загрузкой регистров формирователя при включении питания.

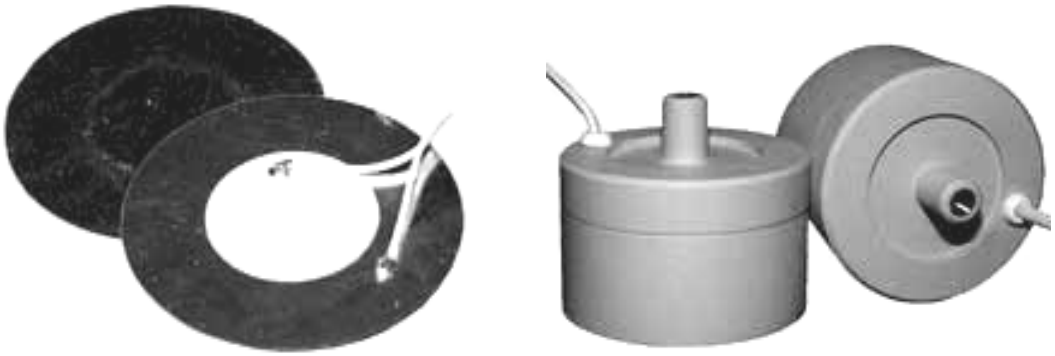
Правильно установленная и отрегулированная система «Соната-АВ» позволяет нейтрализовать такие виды подслушивания как:

- непосредственное подслушивание в условиях плохой звукоизоляции помещения;
- применение радио- и проводных микрофонов, установленных в полостях стен, в надпотолочном пространстве, вентиляционных коробах и т.п.;
- применение стетоскопов, установленных на стенах (потолках, полах), трубах водо- (тепло-, и газо-) снабжения) и т.п.;
- применение лазерных и микроволновых систем съема аудиоинформации с окон и элементов интерьера.

Все генераторные блоки системы имеют входы удаленного беспроводного управления.

Для построения системы защиты помещения требуются виброизлучатели и пьезоизлучатели. Внешний вид излучателей показан на рис. 4.34.

При наладке устанавливается уровень шумового сигнала, который обеспечивает необходимую степень защиты при минимальном акустическом сигнале помехи в помещении, который практически не влияет на комфортность проведения переговоров.



а *б*

Рис. 4.34. Излучатели: *а* – пьезоизлучатели ПИ-45, *б* – виброизлучатели ВИ-45

Параметры «СОНАТА – АВ 1М» представлены в табл. 4.2.

Таблица 4.2

Параметры генератора виброакустических помех «СОНАТА – АВ 1М»

Параметр	Значение
Количество независимых каналов	2
Максимальное количество одновременно подключаемых:	
– виброизлучателей большой мощности (ВИ-45)	20 (10+10)
– аудиоизлучателей (АИ-65)	16 (8+8)
– пьезоизлучателей (ПИ-45)	16 (8+8)
Полоса частот вибрационного и акустического шума гарантированной интенсивности	175–5600 Гц
Превышение вибрационного и акустического шума над уровнем речевого сигнала в канале утечки информации	не менее 10 дБ
Наличие ДУ (интерфейс)	есть, (НР-контакт)
Электропитание изделия	сеть ~220 В / 50 Гц
Условия эксплуатации: – температура окружающей среды – относительная влажность воздуха	 от 5 до 40°С до 80% при t = 25 °С
Продолжительность непрерывной работы изделия	без ограничения

Виброизлучатель ВИ-45 является специализированным электромеханическим преобразователем повышенной мощности и предназначен для возбуждения шумовых вибраций в массивных конструкциях защищаемого помещения, обеспечивая при этом приемлемый уровень мешающего акустического шума. Конструкция и размеры виброизлучателя и элементов его крепления оптимизированы для установки:

– на ограждающих конструкциях помещения (стенах, потолках, полах, дверях);

– на массивных окнах (как на рамах, так и на стеклах);

– на трубах систем тепло-, водо- и газоснабжения.

Виброизлучатель ПИ-45 (пьезоизлучатель) является специализированным электромеханическим преобразователем малой мощности и предназначен для возбуждения шумовых вибраций в стеклах окон (дверей, офисных перегородок).

Варианты крепления виброизлучателей на строительных конструкциях, трубах и стеклах:

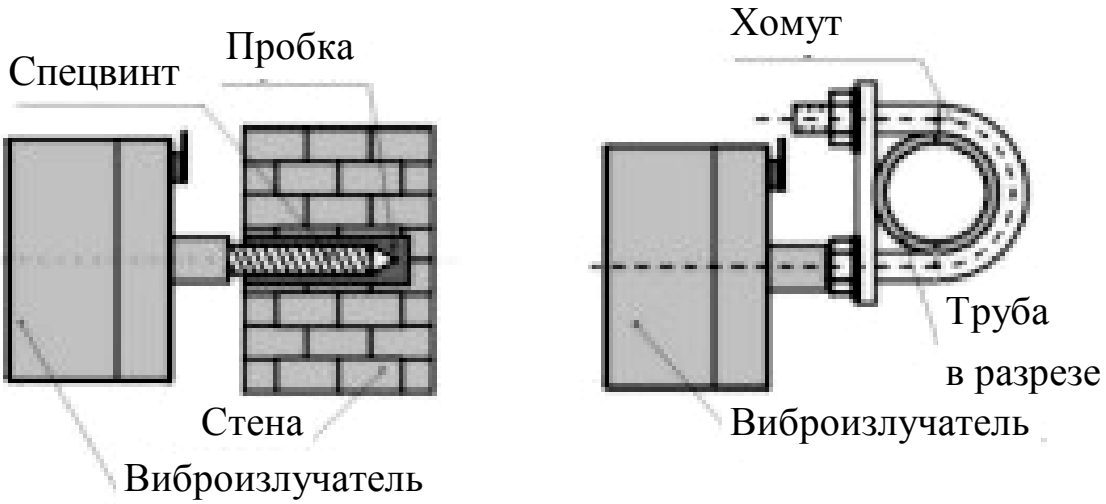


Рис. 4.35. Крепление виброизлучателей

Аудиоизлучатель АИ-65 является специализированным электроакустическим преобразователем и предназначен для возбуждения акустического шума.

Конструкция и размеры аудиоизлучателя и элементов его крепления оптимизированы для его установки:

– в надпотолочном пространстве;

– в вентиляционных каналах;

– дверных тамбурах.

Пример подключения нагрузок к генераторному блоку модели 1А приведен на рис. 4.36.

Рис. 4.36. Подключение нагрузок к генераторному блоку

Мобильный компактный подавитель диктофонов «Мангуст» (рис. 4.37) предназначен для защиты от несанкционированного получения информации при помощи цифровых и кинематических диктофонов.

Рис. 4.37. Подавитель диктофонов «Мангуст»

Устройство не мешает работе радиоэлектронных устройств (например, средств связи), расположенных вне зоны подавления. В отличии от предыдущих моделей имеет малый вес. «Мангуст» является мобильным устройством, предназначенным для установки прицельной помехи и препятствованию функционированию большинства радиоэлектронных приборов, расположенных в зоне подавления. «Мангуст» воздействует на цепи радиоэлектронных устройств высокочастотным сигналом со специальным видом модуляции, который после навязывания обрабатывается в цепях автоматической регулировки усиления совместно с полезным сигналом, значительно превосходя его по уровню и, соответственно, искажая его. Возможно применение прибора для предотвращения утечки информации при помощи проводных микрофонов, а также малогабаритных передатчиков.

Дальность подавления цифровых диктофонов (типа Samsung SVR-820) до 3 м, дальность подавления аналоговых диктофонов (типа Olympus L-400) – до 4 м.

Другие характеристики:

- сектор излучения в горизонтальной плоскости 60°;
- сектор излучения в вертикальной плоскости 127°;
- дистанционное управление по радиоканалу – 2 пульта;
- вес 4,5 кг;
- питание 12 В – от встроенных аккумуляторов;
- время работы – до 40 мин от полностью заряженных аккумуляторов;
- 220 В – опция;
- зарядное устройство в комплекте;
- размер блока 280×195×60, планшета – 350×265×95.

4.10. Скрытие речевой информации в телефонных системах с использованием криптографических методов

Применение криптографических методов защиты информации в телефонных системах существенно повышает стойкость и надежность защиты. Очевидно, что в ближайшем будущем криптографические методы защиты информации в телефонных системах станут основными.

Рассмотрим ряд устройств, обеспечивающих криптографическую защиту в телефонных каналах связи.

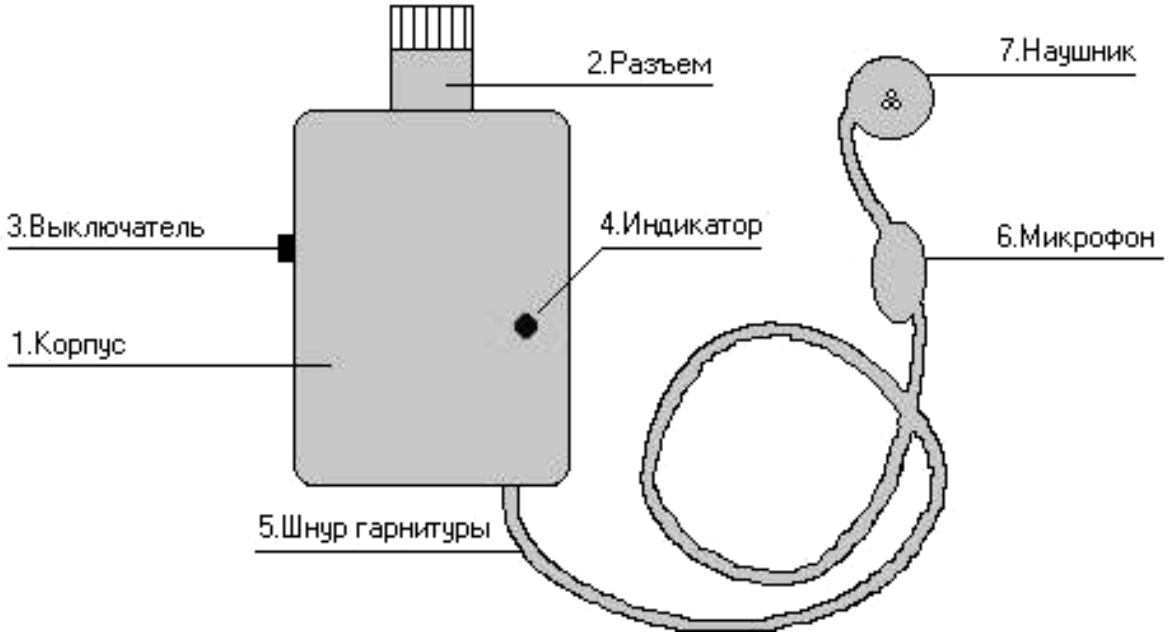


Рис. 4.38. Схема устройства «Альфа-С»

Устройство защиты переговоров в каналах мобильной связи стандарта GSM «Альфа-С» (рис. 4.38) предназначено для защиты речевой информации от несанкционированного доступа. Конструктивно устройство выполнено в виде отдельного блока с гарнитурой и совместимо с мобильными телефонами Siemens.

Устройство кодирования цифрового потока СКРИПТ – 6401 (рис. 4.39) предназначено для защиты информации, передаваемой по каналам связи, образованным цифровыми потоками Е1 путем канального кодирования.

Рис. 4.39. Устройство «Скрипт-6401»

Изделие осуществляет прием линейного сигнала со стороны открытого потока, кодирование информации путем свертки с нелинейным полиномом высокой сложности, формирование и передачу закрытого сигнала в линию, прием линейного сигнала со стороны закрытого потока, раскодирование, формирование и передачу сигнала в направлении открытого потока.

Объектом канального кодирования является поток Е1 с произвольной структурой, в том числе – нефреймированный. Кодированию подвергается вся информация потока Е1, включая информацию сигнализации.

Вид кодирования сигнального уровня (линейный код): HDB3.

На рис. 4.40 приведено типовое включение изделия «Скрипт-6401».

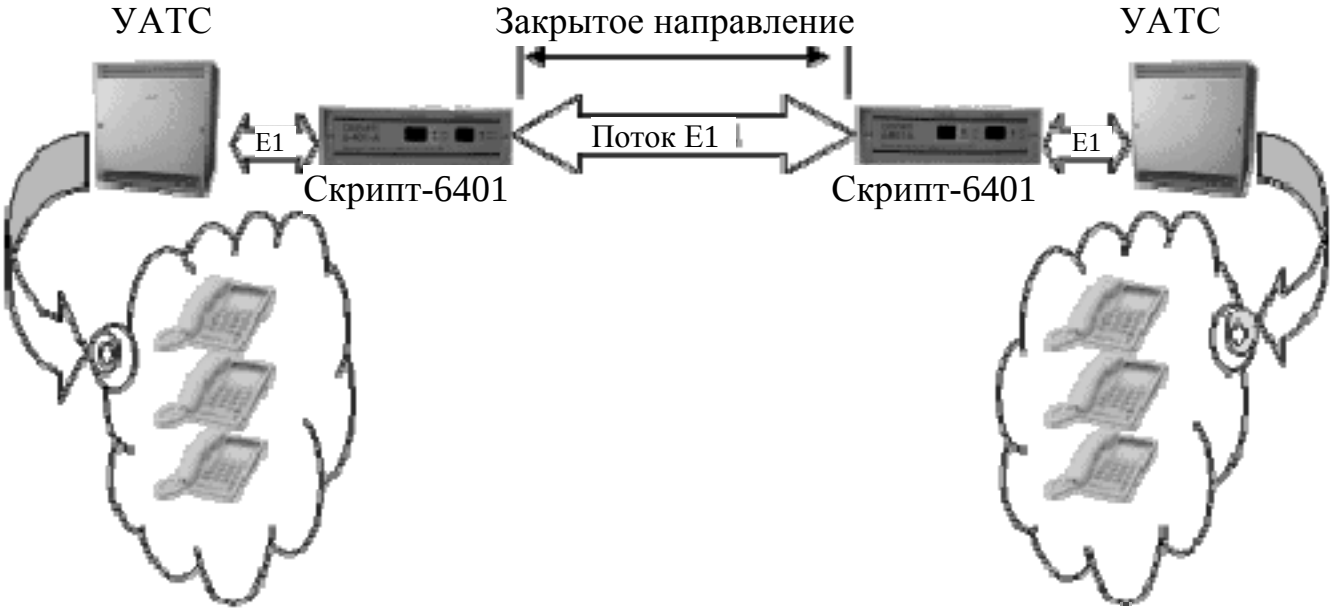


Рис. 4.40. Типовое включение «Скрипт-6401»

Два комплекта изделия включаются в разрыв магистрального кабеля потока Е1. Защите подвергается весь участок с учетом оборудования трансляции без ограничения на протяженность участка..

Протяженность кабеля на участках определяется типом кабеля и составляет на каждом участке не менее 270 м для витой пары.

Рис. 4.41. Приставка «PRAGMA»

Шифратор телефонных каналов связи, факса, ПК PRAGMA (рис. 4.41) предназначено для гарантированной криптографической защиты телефонных каналов связи, факса, ПК. Приставка «PRAGMA» позволяет защитить

от несанкционированного использования документы, базы данных, передаваемые в виде файлов с одного компьютера на другой при помощи модема. Устройство при этом включается вместо обычного модема и работает под управлением стандартного коммуникационного пакета на ПЭВМ в режиме для выделенной линии.

Особенности прибора:

- Автономное питание.
- Высокая стойкость.
- Усиленная ключевая система – 1024 бит.
- Возможность оперативной смены мастер-ключа пользователем.
- Автономное питание.
- Возможность построение конфиденциальной связи в необходимом месте.
- Оптимизирован для работы на «дальних» каналах связи (международных, спутниковых).
- Симметричное шифрование по ГОСТ 28147-89.
- Алгоритм речепреобразования – CELP 4800 бод.
- Защита факсимильных документов путем шифрования передаваемого изображения, в защищенный факсимильный документ добавляется «шапка», внешний вид которой может задавать сам пользователь.
- Защита факсимильных документов происходит автоматически, не требуя вмешательства пользователя.
- Защита межкомпьютерного обмена данными.
- Система открытого распределения ключей Диффи-Хеллмана (1024 бит) создает уникальный ключ для каждого сеанса связи и исключает необходимость ввода сеансовых ключей пользователем;
- Система проверки подлинности, исключающая возможность вмешательства «третьей» стороны (атаки вида «человек посредине»), даже при наличии подобного устройства. Решается это применением алгоритмов «защищенные переговоры о согласовании ключа».
- Возможность смены ключевых и др. параметров работы устройства самим пользователем.
- Возможность оперативной смены ключевых параметров (предусмотрен инжектор ключей, позволяющий менять ключевые параметры устройства). При этом осуществляется проверка на целостность ключевых параметров, предотвращающая несанкционированное навязывание параметров ключевой системы.
- Исключение возможности влияния производителя устройства на систему защиты, организуемой пользователем.

«PRAGMA» представляет собой шифратор нового поколения, позволяющий создавать конфиденциальные сети связи с защитой всего канала,

от одного шифратора до другого, предотвращает прослушивание речевых переговоров, перехват факсимильных документов и передаваемых данных при межкомпьютерном обмене. Максимальное количество абонентов сети неограниченно.

Качество восстановленного (синтезированного) сигнала практически не отличается, а во многих случаях выше обычного открытого.

«PRAGMA» выполнен в виде приставки к телефонному (факсимильному) аппарату и подключается между телефонной линией и телефоном. Для передачи данных устройство соединяется с компьютером по последовательному коммуникационному порту (COM).

При защите факсимильных документов шифруется само изображение, передаваемое на скоростях 2400–9600 бит/с. При этом сигналы в телефонной линии не отличаются от обычной факсимильной передачи.

Для построения системы защищенной связи необходимы как минимум два устройства «PRAGMA». Приставки включаются в разрыв между телефонным (факсимильным) аппаратом и телефонной линией у каждого абонента и обеспечивают защиту от прослушивания в открытом канале связи на участке от одного устройства до другого.

При включении питания осуществляется самотестирование устройства и переход в режим ожидания. О правильной работе в режиме ожидания свидетельствует поочередное включение/выключение индикаторов режимов работы. В таком состоянии (а так же при выключенном питании) приставка «прозрачна» для всех операций с телефонным (факсимильным) аппаратом и не мешает обычной работе пользователя.

Перевод устройства в режим защиты переговоров должен производиться после установления связи между абонентами и может осуществляться несколькими способами:

- нажатием кнопки;
- набором определенной комбинации цифр (символов) с клавиатуры телефонного аппарата в режиме тонального набора;
- устройство может включаться автоматически при обнаружении служебных посылок со стороны второго абонента.

Переход в режим открытой связи (ожидания) осуществляется нажатием соответствующей кнопки или автоматически, при переключении в открытый режим противоположного абонента. Если ложится трубка телефонного аппарата, приставка отключается и возвращается в режим ожидания.

Защита факсимильных документов осуществляется без вмешательства пользователя. Устройство включается при обнаружении начала факсимильной процедуры, шифрует передаваемый документ (дешифрует принимаемый) при наличии такой же приставки (с таким же ключом) с противоположной стороны и возвращается в режим ожидания.

Защищенный документ помечается специальной строкой в начале каждой страницы.

Предусмотрена возможность блокирования приема и/или передачи факсимильного документа в незащищенном режиме.

Устройство защиты речевой и факсимильной информации в открытых каналах связи ALT-4132M (рис. 4.42) предназначено для предотвращения прослушивания речевых переговоров, перехвата факсимильных документов.

ALT-4132M выполнен в виде приставки к телефонному (факсимильному) аппарату и подключается между телефонной линией и телефоном. Защита речевой информации осуществляется путем вокодерного преобразования и шифрования по алгоритму ГОСТ28149-89 с высокой стойкостью к вскрытию.

Рис. 4.42. Устройство «ALT-4132M»

Аппарат может эксплуатироваться с факс-машинами и факс-модемами группы 3 (ISO, G3).

Обеспечивается гальваническая развязка с линией и телефонным (факсимильным) аппаратом.

Обеспечивается передача и прием факсимильных документов без снижения скорости по сравнению с открытой передачей согласно рекомендациям ITU.T (T.30, T.4, V.27ter-2400, V27ter-4800, V.29-7200, V.29-9600).

Сигналы в линии при работе устройства в режиме защиты факсимильных сообщений не отличаются от сигналов стандартной факсимильной процедуры.

Рис. 4.43. Устройство «УКС-001»

В устройстве защиты переговоров УКС-001 (рис. 4.43) реализован абонентский метод шифрования в каналах сотовой связи стандарта GSM 900/1800 на базе созданного криптографического устройства конфиденциальной связи УКС-001.

УКС-001 совместно с подключенным к нему мобильным телефоном Ericsson-R520m обеспечивает проведение сеансов защищённых переговоров по каналу передачи данных.

Криптографическая стойкость защищённого УКС-001 канала связи подтверждена государственной экспертизой.

Основные свойства устройства:

- Время непрерывной работы в режиме секретной связи не менее 4 ч, в режиме ожидания – не менее 100 ч.
- Размер секретного ключа шифрования 256 бит.
- Загрузка секретных ключей в память УКС-001 на каждые 30 дней переговоров производится в центре сопровождения или самим пользователем 1 раз в месяц.
- Для повышения степени защищённости пользователей устройство автоматически производит ежедневную смену секретных ключей.
- Отсутствует возможность использования УКС-001 другим лицом в случае его утери.

Устройство маскирования телефонных сообщений (УМТС) в каналах GSM связи РЕЗЕДА (рис.4.44) предназначено для защиты телефонных сообщений, передаваемых между мобильными радиотелефонами сотовых сетей стандарта GSM, от несанкционированного доступа (НСД) к их содержимому.

Рис. 4.44. Устройство «РЕЗЕДА»

Защита телефонных сообщений от НСД обеспечивается путем изменения по определенному, неизвестному для потенциального злоумышленника, правилу спектра передаваемого сигнала.

Такое техническое решение исключает оперативный перехват телефонных переговоров, т.к. для восстановления телефонных сообщений требует применения специальной аппаратуры и осуществления временных затрат подготовленных специалистов порядка 150 ч.

УМСТ размещается в специально изготовленном металлическом контейнере размером 43×15×11 мм, с одной стороны к которому подключена микротелефонная гарнитура, а с другой стороны – кабель с разъемом, с помощью которого УМСТ штатно подключается к радиотелефону. Для питания УМСТ используется аккумуляторная батарея радиотелефона.

Рис. 4.45. Устройство «OPEX-2»

Устройство защиты речевой информации в открытых каналах связи OPEX-2 (рис. 4.45) предназначено для организации засекречивающей связи с высокой степенью защищенности от несанкционированного восстановления информации, передаваемой по коммутируемым или выделенным каналам связи с 2-х проводным абонентским окончанием.

Защита речевой информации осуществляется методом частотно-временного скремблирования. Устройство обеспечивает уникальный ключ на каждый сеанс связи и возможность аутентификации с использованием пароля, вводимого с телефонного аппарата, управление одной кнопкой. Использует систему открытого распределения ключей Диффи-Хеллмана.

Закрытие речевой информации достигается следующими методами: временных перестановок; инверсии спектра сигнала; преобразования временного масштаба, разрушающего непрерывность речевого сигнала.

Стойкость защиты информации к несанкционированному вскрытию обеспечивается трехуровневой ключевой системой, включающей в себя: пароль – предназначен для идентификации абонентов, входящих в связь, вводится с клавиатуры телефонного аппарата, подключенного к приставке, содержит четыре цифры (используется при необходимости); мастер-ключ разрядностью 128 бит – для заказываемой партии телефонных приставок (размещается в постоянном запоминающем устройстве); сеансовый ключ – генерируется физическим датчиком случайный чисел и имеет разрядность 128 бит.

Обмен сеансовыми ключами в приставке реализован по методу открытого распределения ключей с генерацией разовых ключей для каждого сеанса связи. Ключ формируется от физического датчика случайных чисел и является уникальным для каждого сеанса связи. Сформированный ключ является достаточным для установления надежной защиты, однако, дополнительно предусмотрена возможность аутентификации с помощью пароля, который может вводиться пользователем с клавиатуры телефонного аппарата. Пароль может использоваться, например, для организации иерархической структуры, когда пользователю высшего звена известны все пароли структуры, и он имеет возможность связываться со всеми звеньями, а пользователь низшего звена, зная лишь свой пароль, работает только на своем уровне.

4.11. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах

4.11.1. Secret Net 5.0

Secret Net 5.0 [50] – это система защиты конфиденциальной информации от несанкционированного доступа нового поколения, которая реализует требования руководящих документов и ГОСТ по защите информации и функционирует под управлением современных ОС MS Windows 2000, Windows XP и Windows 2003. Существует в автономном и сетевом вариантах.

За счёт интеграции собственных защитных механизмов с механизмами управления сетевой инфраструктуры защищаемой сети Secret Net 5.0 по-

вышает защищенность всей автоматизированной информационной системы в целом и при этом [50]:

- обеспечивает централизованное управление настройками политики безопасности;
- работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты;
- осуществляет мониторинг и аудит политики безопасности в режиме реального времени;
- позволяет оперативно реагировать на события НСД;
- поддерживает терминальный режим работы пользователей с рабочей станцией.

Структура Secret Net 5.0 показана на рис. 4.46.

Рис. 4.46. Структура Secret Net 5.0

Интеграция системы управления Secret Net 5.0 со штатным механизмами управления информационной системой позволяет избежать постоянно возникающих проблем синхронизации данных между ИС и выделенным сервером настроек, который имелся в предыдущих версиях системы и часто присутствует в аналогичных системах защиты.

Система обеспечивает:

- оперативное реагирование на действия злоумышленников;
- централизованный просмотр событий безопасности;
- контроль вывода конфиденциальной информации на внешние носители;
- аппаратную идентификацию пользователей;
- централизованное управление;
- контроль целостности файлов;

• разграничение доступа к устройствам (CD\DVD, USB, Wi-Fi и т.д.).

Secret Net 5.0 (сетевой вариант) содержит следующие компоненты:

• клиент Secret Net 5.0;

• сервер безопасности Secret Net 5.0;

• программу оперативного управления, мониторинга и аудита («Монитор»);

• модификатор схемы Active Directory.

Клиент

Клиент Secret Net 5.0 следит за соблюдением настроенной политики безопасности на рабочих станциях и серверах, обеспечивает регистрацию событий безопасности и передачу журналов на Сервер Безопасности, а также приём от него оперативных команд и их выполнение.

Сервер безопасности

Сервер безопасности производит сбор журналов от зарегистрированных на нем агентов, накапливает полученную информацию в базе данных и обеспечивает выдачу команд оперативного управления клиентам (например, блокировку рабочей станции при выявлении попытки НСД).

Программа оперативного управления, мониторинга и аудита («Монитор»)

Монитор является программой, которая отображает администратору оперативную информацию от Сервера Безопасности о состоянии рабочих станций и дает возможность отслеживать:

• какие компьютеры сети в данный момент включены;

• какие пользователи на них работают (как локально, так и в терминальном режиме).

«Монитор» в режиме реального времени отображает оперативную информацию о происходящих событиях НСД, позволяет осуществлять просмотр журналов всех рабочих станций, а также выдавать на защищаемые рабочие станции команды оперативного управления.

Модификатор схемы Active Directory

Модификатор схемы Active Directory (AD) используется для подготовки схемы ОС Windows к развертыванию Secret Net 5.0. Так как в качестве хранилища информации о настройках безопасности Secret Net 5.0 использует AD, данный модуль создаёт новые объекты и изменяет параметры существующих. Программы управления объектами и параметрами групповых политик, входящие в состав этого модуля, обеспечивают управление параметрами работы доменных пользователей и применение централизованных настроек безопасности Secret Net 5.0.

Управление системой Secret Net 5.0

Система централизованного управления

В качестве хранилища информации в системе централизованного управления используется Active Directory (AD). Для нужд централизован-

ного управления Secret Net 5.0 схема Active Directory расширяется – создаются новые объекты и изменяются параметры существующих.

Для выполнения этих действий используется специальный модуль изменения схемы AD, который устанавливается и запускается на контроллере домена при установке системы централизованного управления. Для приведения параметров работы защитных средств компьютера в соответствие настройкам безопасности Secret Net 5.0, задаваемым с помощью групповых политик, используется агент Secret Net 5.0, установленный на каждом сервере или рабочей станции защищаемой сети.

Столь тесная интеграция системы управления с Active Directory позволяет легко использовать Secret Net 5.0 для организации защиты сети, использующей многодоменную структуру.

Оперативный мониторинг и аудит

В Secret Net 5.0 предусмотрена функция оперативного мониторинга и аудита безопасности информационной системы предприятия, которая позволяет решать такие задачи, как:

- оперативный контроль состояния автоматизированной системы предприятия (получение информация о состоянии рабочих станций и о работающих на них пользователях);
- централизованный сбор журналов с возможностью оперативного просмотра в любой момент времени, а также хранение и архивирование журналов;
- оповещение администратора о событиях НСД в режиме реального времени;
- оперативное реагирование на события НСД – выключение, перезагрузка или блокировка контролируемых компьютеров;
- ведение журнала НСД.

Система оперативного управления имеет свою базу данных, в которой хранится вся информация, связанная с работой сервера по обеспечению взаимодействия компонентов, а также журналы, поступающие от агентов.

В качестве базы данных используется СУБД Oracle 9i.

Мониторинг

С помощью программы мониторинга администратор может управлять сбором журналов с рабочих станций. Предусмотрено два варианта. Первый – сервер оперативного управления собирает журналы по команде администратора. Второй – администратор составляет расписание и передает его серверу, далее сервер собирает журналы в соответствии с этим расписанием.

Также предусмотрена возможность создать удобный для администратора вид представления сети – так называемый «срез» (например, по отделам, по территориальному размещению и т.п.). В случае крупной распределённой сети эта функция делегируется другим администраторам для управления выделенными им сегментами сети.

Аудит

Программа работы с журналами устанавливается на рабочем месте сотрудника, уполномоченного проводить аудит системы защиты. Если функции мониторинга и аудита совмещает один сотрудник, программа устанавливается на том же компьютере, который является рабочим местом администратора оперативного управления.

В системе Secret Net 5.0 для проведения аудита используются 4 журнала:

- журнал приложений;
- журнал безопасности;
- журнал системы;
- журнал Secret Net.

Первые три из перечисленных журналов – штатные, входящие в состав средств операционной системы. В журнале Secret Net хранятся сведения о событиях, происходящих в системе Secret Net 5.0.

Журналы ведутся на каждом защищаемом компьютере сети и хранятся в его локальной базе данных. Сбор журналов осуществляется по команде аудитора или по расписанию.

Программа работы с журналами позволяет аудитору просматривать записи журналов и тем самым отслеживать действия пользователей, связанные с безопасностью автоматизированной информационной системы предприятия.

В программе управления журналами предусмотрена настраиваемая выборка записей, используя которую аудитор может просматривать не весь журнал целиком, а только часть записей, удовлетворяющих определенным критериям. Это значительно ускоряет и упрощает работу, связанную с поиском и анализом событий.

С помощью программы работы с журналами аудитор может выдавать команды серверу на архивацию журналов, а также на восстановление журналов из архива. Предусмотрена возможность просмотра архивов, а также сохранения журнала в файл для последующей передачи и анализа записей вне системы Secret Net 5.0.

Защитные механизмы

Усиленная идентификация и аутентификация пользователей

Система Secret Net 5.0 совместно с ОС Windows обеспечивает усиленную идентификацию и аутентификацию пользователя с помощью средств аппаратной поддержки при его входе в систему, а также позволяет существенно снизить риски того, что пользователь загрузит компьютер с отчуждаемых внешних носителей и получит доступ к важной информации в обход системы защиты.

В качестве аппаратной поддержки система Secret Net 5.0 использует: программно-аппаратный комплекс «Соболь» и Secret Net Touch Memory

Card. Плату аппаратной поддержки невозможно обойти средствами BIOS. Если в течение определённого времени после включения питания на плату не было передано управление, она блокирует работу всей системы.

Полномочное управление доступом

Каждому информационному ресурсу назначается один их трёх уровней конфиденциальности: «Не конфиденциально», «Конфиденциально», «Строго конфиденциально», а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.

Разграничение доступа к устройствам

Функция обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера. Существует возможность запретить, либо разрешить пользователям работу с любыми портами\устройствами.

Разграничивается доступ к следующим портам/устройствам:

- последовательным и параллельным портам;
- сменным, логическим и оптическим дискам;
- USB – портам.

Также поддерживается контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей.

Существует возможность запретить использование сетевых интерфейсов – Ethernet, 1394 FireWire, Bluetooth, IrDA, WiFi.

Замкнутая программная среда

Для каждого пользователя компьютера формируется определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, «червей» и шпионского ПО, а также использования ПК в качестве игровой приставки.

Контроль целостности

Используется для слежения за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути. При обнаружении несоответст-

вия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

- регистрация события в журнале Secret Net;
- блокировка компьютера;
- восстановление повреждённой/модифицированной информации;
- отклонение или принятие изменений.

Гарантированное уничтожение данных

Уничтожение достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено до 10 циклов (проходов) затирания.

Контроль аппаратной конфигурации компьютера

Осуществляет своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирования на эти изменения.

Предусмотрено два вида реакций:

- регистрация события в журнале Secret Net;
- блокировка компьютера.

Контроль печати конфиденциальной информации

Администратор безопасности имеет возможность запретить вывод конфиденциальной информации на печать, либо разрешить эту операцию некоторым пользователям, при этом распечатанные документы могут автоматически маркироваться в соответствии с правилами оформления документов. Также сам факт печати (или попытки несанкционированного вывода на печать) отображается в журнале защиты Secret Net 5.0.

Регистрация событий

Система Secret Net 5.0 регистрирует все события, происходящие на компьютере: включение\выключение компьютера, вход\выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.

Функциональный самоконтроль подсистем

Самоконтроль производится перед входом пользователя в систему и предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 5.0 загружены и функционируют.

Импорт и экспорт параметров

В Secret Net 5.0 реализована возможность экспорта и импорта различных параметров системы. После проверки корректности работы защитных механизмов на компьютере, принимаемом за эталонный, выполняется экспорт значений параметров в файл. Далее значения импортируются на необходимое количество компьютеров.

4.11.2. Электронный замок «СОБОЛЬ»

Среди средств так называемых AAA (authentication, authorization, administration – аутентификация, авторизация, администрирование) важное место занимают программно-аппаратные инструменты контроля доступа к компьютерам – электронные замки, устройства ввода идентификационных признаков (УВИП) и соответствующее программное обеспечение (ПО). В этих средствах контроля доступа к компьютерам идентификация и аутентификация, а также ряд других защитных функций, выполняются с помощью электронного замка и УВИП до загрузки ОС.

По способу считывания современные УВИП подразделяются на контактные, дистанционные и комбинированные.

Контактное считывание идентификационных признаков осуществляется непосредственным взаимодействием идентификатора и считывателя.

При бесконтактном способе считывания идентификатор может располагаться на некотором расстоянии от считывателя, а сам процесс считывания осуществляется радиочастотным или инфракрасным методом.

УВИП могут быть электронными, биометрическими и комбинированными.

Электронные УВИП содержат микросхему памяти идентификационного признака.

Примером электронного замка может служить устройство «СОБОЛЬ» (рис. 4.47).

Рис. 4.47. Электронный замок «Соболь-PCI»

Назначение

Применяется для защиты ресурсов компьютера от несанкционированного доступа.

Электронный замок «Соболь-PCI» сертифицирован Гостехкомиссией России. Сертификат подтверждает соответствие данного изделия требованиям Руководящего документа Гостехкомиссии России «Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации» и позволяет использовать данный продукт при разработке систем защиты для автоматизированных систем с классом защищенности до 1В включительно.

Применение

Электронный замок «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

Электронный замок «Соболь» обладает следующими возможностями:

- идентификация и аутентификация пользователей;
- регистрация попыток доступа к ПЭВМ;
- запрет загрузки ОС со съемных носителей;
- контроль целостности программной среды.

Возможности по идентификации и аутентификации пользователей, а также регистрация попыток доступа к ПЭВМ не зависят от типа использующейся ОС.

Идентификация и аутентификация пользователей

Каждый пользователь компьютера регистрируется в системе электронный замок «Соболь», установленной на данном компьютере. Регистрация пользователя осуществляется администратором и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора и назначении пароля.

Действие электронного замка «Соболь» состоит в проверке персонального идентификатора и пароля пользователя при попытке входа в систему. В случае попытки входа в систему не зарегистрированного пользователя электронный замок «Соболь» регистрирует попытку НСД и осуществляется аппаратная блокировка до 4-х устройств (например: FDD, CD-ROM, ZIP, LPT, SCSI-порты).

В электронном замке «Соболь» используются идентификаторы Touch Memory фирмы Dallas Semiconductor. Загрузка операционной системы с жесткого диска осуществляется только после предъявления зарегистрированного идентификатора. Служебная информация о регистрации пользователя (имя, номер присвоенного персонального идентификатора и т.д.) хранится в энергонезависимой памяти электронного замка.

Регистрация попыток доступа к ПЭВМ

Электронный замок «Соболь» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Электронный замок «Соболь» фиксирует в системном журнале вход пользователей, попытки входа, попытки НСД и другие события, связанные с безопасностью системы.

В системном журнале хранится следующая информация: дата и время события, имя пользователя и информация о типе события, например:

- факт входа пользователя;
- введение неправильного пароля;
- предъявление не зарегистрированного идентификатора пользователя;
- превышение числа попыток входа в систему;
- другие события.

Таким образом, электронный замок «Соболь» предоставляет информацию администратору о всех попытках доступа к ПЭВМ.

Контроль целостности программной среды и запрет загрузки со съемных носителей

Подсистема контроля целостности расширяет возможности электронного замка «Соболь». Контроль целостности системных областей дисков и наиболее критичных файлов производится по алгоритму ГОСТ 28147-89 в режиме имитовставки. Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов. Подсистема запрета загрузки с гибкого диска и CD ROM диска обеспечивает запрет загрузки операционной системы с этих съемных носителей для всех пользователей компьютера, кроме администратора. Администратор может разрешить отдельным пользователям компьютера выполнять загрузку операционной системы со съемных носителей.

Подсистемы контроля целостности и подсистемы запрета загрузки со съемных носителей функционируют под управлением следующих ОС:

MS DOS версий 5.0-6.22 (только ЭЗ «Соболь» для стандарта ISA); ОС семейства Windows'9x (FAT12, FAT16 или FAT32); Windows NT версий 3.51 и 4.0 с файловой системой NTFS; Windows 2000 с файловой системой NTFS (только «Соболь-PCI»); UNIX FreeBCD (только «Соболь-PCI»).

Возможности по администрированию

Для настройки электронного замка «Соболь» администратор имеет возможность:

- определять минимальную длину пароля пользователя;
- определять предельное число неудачных входов пользователя;
- добавлять и удалять пользователей;
- блокировать работу пользователя на компьютере;
- создавать резервные копии персональных идентификаторов.

Использование

Электронный замок «Соболь» может применяться в составе системы защиты информации Secret Net для генерации ключей шифрования и электронно-цифровой подписи. Кроме того, при использовании ЭЗ «Соболь» в составе СЗИ Secret Net обеспечивается единое централизованное управление его возможностями. С помощью подсистемы управления Secret Net администратор безопасности имеет возможность управлять статусом персональных идентификаторов сотрудников: присваивать электронные идентификаторы, временно блокировать, делать их недействительными, что позволяет управлять доступом сотрудников к компьютерам автоматизированной системы организации.

4.11.3. USB-ключ

Основное технологическое отличие USB-ключа от смарт-карты заключается в том, что хранимая в памяти USB-ключа информация не привязана жестко к ячейкам памяти, а располагается в специальной файловой системе. Поэтому один и тот же ключ можно использовать для разных целей: для входа в компьютер, авторизации электронной почты, создания канала виртуальной частной сети (VPN – virtual private network) и многого другого. Таким образом, с помощью одного аппаратного ключа можно комплексно решить задачу идентификации пользователя для всего комплекса офисного программного обеспечения. При этом человек не должен знать пароли и ключи шифрования для всех приложений, достаточно одного пароля для работы с ключом.

Для повышения надежности защиты некоторые аппаратные ключи выполнены в герметичном, влагостойком и пыленепроницаемом корпусе, что гарантирует защищенность данных от многих внешних воздействий. При разгерметизации корпуса информация из памяти ключа стирается. Это сделано для того, чтобы блокировать копирование или подделку ключа и обеспечить достаточно надежное хранение информации внутри аппаратного идентификатора при более жестких требованиях к его конструктиву. Реализовать те же самые требования для всего компьютера значительно сложнее.

Назначение USB-ключа:

- строгая двухфакторная аутентификация пользователей при доступе к защищённым ресурсам (компьютерам, сетям, приложениям);
- аппаратное выполнение криптографических операций в доверенной среде (в электронном ключе: генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, выработка ЭЦП);
- безопасное хранение криптографических ключей, профилей пользователей, настроек приложений, цифровых сертификатов и пр. в энергонезависимой памяти ключа;
- поддержка большинством современных операционных систем, бизнес приложений и продуктов по информационной безопасности в качестве средства аутентификации и авторизации.

Возможности применения USB-ключа:

- строгая аутентификация пользователей при доступе к серверам, базам данных, разделам веб сайтов;
- безопасное хранение секретной информации: паролей, ключей ЭЦП и шифрования, цифровых сертификатов;
- защита электронной почты (цифровая подпись и шифрование, доступ);

- защита компьютеров;
- защита сетей, VPN;
- клиент-банк, домашний банк;
- электронная торговля.

Преимущества

USB-ключ, может использоваться в любых приложениях для замены парольной защиты на более надежную двухфакторную аутентификацию (когда пользователь имеет нечто – USB-ключ, и знает нечто – PIN код).

USB-ключ обеспечивает:

- строгую аутентификацию пользователей за счет использования криптографических методов;
- безопасное хранение ключей шифрования и ЭЦП (электронной цифровой подписи), а также цифровых сертификатов для доступа к защищенным корпоративным сетям и информационным ресурсам;
- мобильность для пользователя и возможность работы в «не доверенной среде» (например, с чужого компьютера) – за счет того, что ключи шифрования и ЭЦП генерируются в памяти USB-ключ аппаратно и не могут быть перехвачены;
- безопасное использование – воспользоваться им может только его владелец, знающий PIN-код;
- реализацию как российских, так и западных стандартов шифрования и ЭЦП;
- удобство работы – USB-ключ выполнен в виде брелока со световой индикацией режимов работы и напрямую подключается к USB-портам, которыми сейчас оснащаются 100% компьютеров, не требует специальных считывателей, блоков питания, проводов и т.п.;
- использование одного ключа для решения множества различных задач – входа в компьютер, входа в сеть, защиты канала, шифрования информации, ЭЦП, безопасного доступа к защищённым разделам Web-сайтов, информационных порталов и т.п.

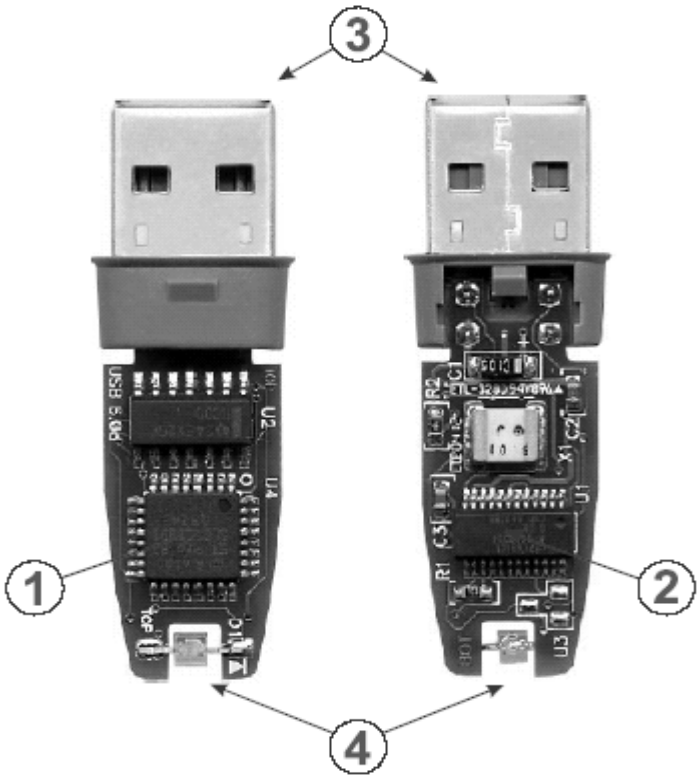


Рис. 4.48 . USB-ключ

USB-ключ имеет (рис. 4.48):

- микросхему (1);

- защищенный микроконтроллер (2);
- разъем USB (3);
- световой индикатор режимов работы (4);
- герметичный полупрозрачный пластиковый корпус.

Микроконтроллер в составе USB-ключа обеспечивает:

- коммуникационные функции (поддержку протокола USB);
- хранение микрокода для управления протоколом передачи (firmware).

В состав микросхемы входят:

- 16-ти битный центральный процессор с набором инструкций;
- память только для чтения (ROM, Read Only Memory), содержащая операционную систему;
- оперативная память (RAM, Random Access Memory), предназначенная для использования операционной системой;
- электрически стираемая программируемая память только для чтения (EEPROM, Electrically Erasable Programable Read Only Memory), предназначенная для хранения пользовательских данных;
- аппаратный генератор случайных чисел;
- криптопроцессор для ускорения выполнения криптографических операций.

4.11.4. Считыватели «Proximity»

Технология Proximity прочно завоевала ведущее место в профессиональных системах управления доступом, потеснив магнитные и Wiegand считыватели и практически полностью вытеснив Touch memory.

Устройства ввода идентификационных признаков на базе идентификаторов Proximity (от английского слова proximity – близость, соседство) относится к классу электронных бесконтактных радиочастотных устройств.

Они выпускаются в виде карточек, ключей, брелоков и т.п. Каждый из них имеет собственный уникальный серийный номер. Основными составляющими устройств являются интегральная микросхема для связи со считывателем и встроенная антенна. В составе микросхемы находятся приемопередатчик и запоминающее устройство, хранящее идентификационный код и другие данные. Внутри Proximity может быть встроена литиевая батарейка (активные идентификаторы). Активные идентификаторы могут считывать информацию на расстоянии нескольких метров. Расстояние считывания пассивными идентификаторами (не имеющих батарейки) составляет десятки сантиметров.

Устройство считывания постоянно излучает радиосигнал, который принимается антенной и передается на микросхему. За счет принятой энер-

гии идентификатор излучает идентификационные данные, принимаемые считывателем.

Рассмотрим принципы работы считывателей «Parsec».

Считыватели Proximity в своей работе опираются на широко известные физические принципы. Правда, того же нельзя сказать об алгоритмах обработки сигналов в схеме считывателя, что обычно и составляет «ноу хау» производителей. Рис. 4.49 поясняет взаимодействие карты и считывателя в процессе получения кода, заносимого в карту при ее производстве.

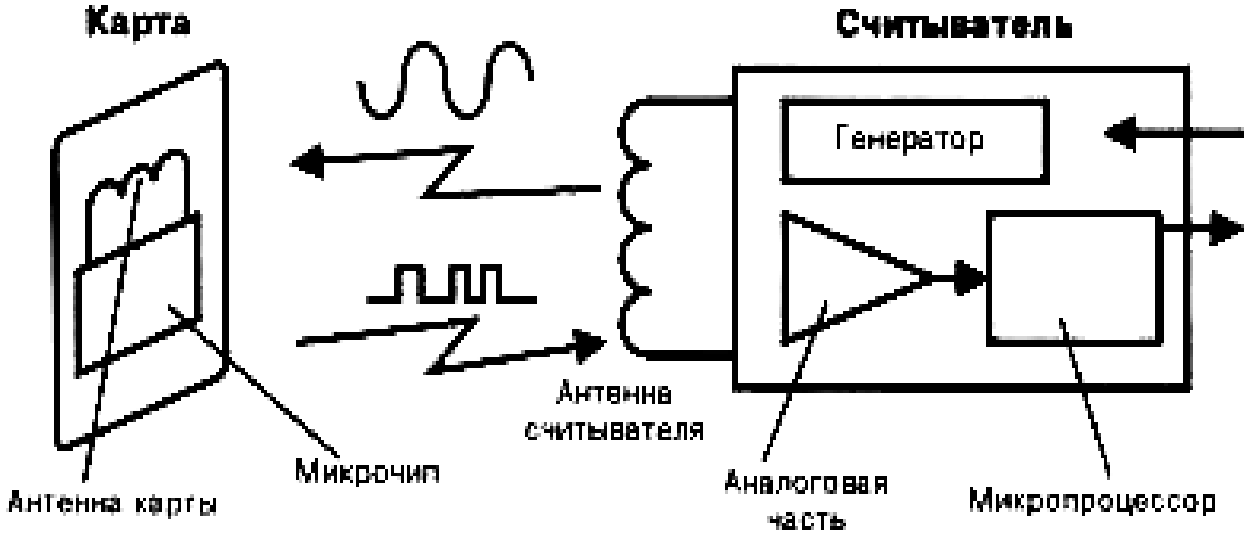


Рис. 4.49. Принцип работы Proximity считывателя

Считыватель содержит генератор, работающий, как правило, на частоте 125 кГц, и нагруженный на антенну считывателя. Излучаемая антенной считывателя энергия принимается антенной карты и запитывает расположенный в карте микрочип. Последний модулирует сигнал в антенне карты кодом, занесенным в микрочип на заводе-изготовителе. Излученный картой сигнал воспринимается антенной считывателя, обрабатывается сначала аналоговой частью схемы считывателя, а затем расположенным в считывателе микропроцессором. Микропроцессор проверяет корректность кода, преобразовывает его к требуемому формату и выдает на выход считывателя, то есть на вход контроллера системы управления доступом.

При всем многообразии форматов данных, обрабатываемых контроллерами систем управления доступом, более 80% систем ориентируются в качестве основного или дополнительного на формат Wiegand 26 бит.

Другой популярный формат интерфейса систем управления доступом – формат шины Micro LAN американской фирмы Dallas, в соответствии с которым работают ключи Touch memory. В отличие от Wiegand 26 этот формат хорошо документирован фирмой в литературе, поэтому не будем приводить его описание.

Почти все российские разработчики систем управления доступом ориентировались именно на использование протокола Micro LAN в своих контроллерах.

Считыватели «Parsec»

Под торговой маркой «Parsec» производится достаточно широкий спектр оборудования систем управления доступом. В частности, это автономные контроллеры серии ASC-xx и сетевая компьютеризированная система управления доступом ParsecLight. Вместе с тем под этой торговой маркой продается целая гамма Proximity считывателей для применения в существующих системах как отечественного, так и зарубежного производства.

Внешний вид считывателей APR-O3xx, APR-04xx и APR-05xx показан на рис. 4.50.

Рис. 4.50. Внешний вид считывателей «Parsec»

Особо следует сказать о считывателе APR-05xx, который выполнен в корпусе из нержавеющей стали и предназначен для уличной установки в случаях, когда требуется повышенная защита от вандализма.

4.11.5. Технология защиты информации на основе смарт-карт

Появление информационной технологии смарт-карт (СК), основанной на картах со встроенным микропроцессором, позволило удобнее решать вопросы использования пластиковых денег. Однако уникальные возможности СК с микропроцессором, состоящие в высокой степени защиты от подделки, поддержке базовых операций по обработке информации, обеспечении высоких эксплуатационных характеристик, сделали СК одним из лидеров среди носителей конфиденциальной информации.

Следует отметить отличительные особенности таких карт. СК содержит микропроцессор и ОС, которые обеспечивают уникальные свойства защиты, имеют контактное и бесконтактное исполнение (на рис. 4.51 показана бесконтактная смарт-карта).

Таким образом, технология СК обеспечивает надежное хранение ключей и доступ к различным информационным ресурсам.

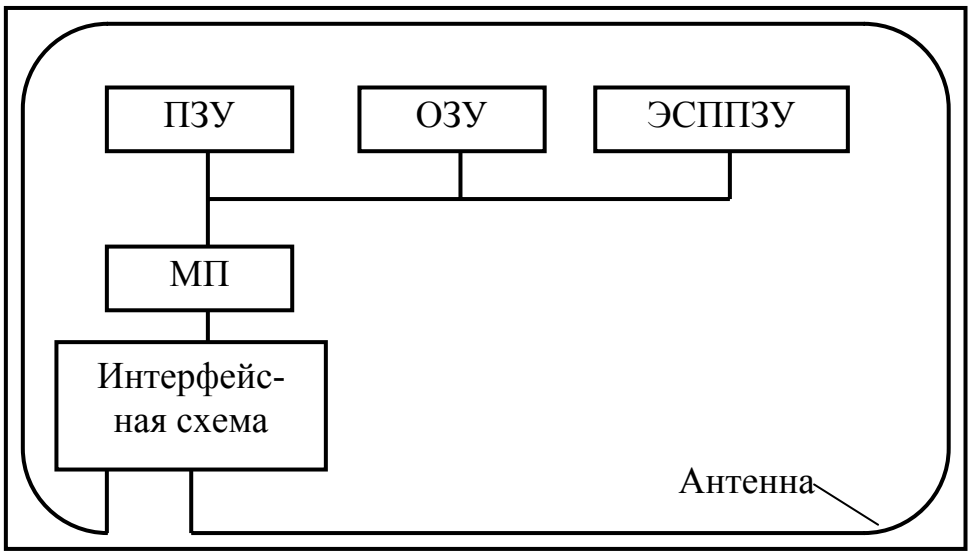


Рис. 4.51. Схема бесконтактной смарт-карты

Персональные идентификаторы iKey компании Rainbow являются недорогими брелоками, которые могут использоваться на любой рабочей станции, имеющей универсальную последовательную шину (USB). Они обеспечивают надежность, простоту и безопасность в такой же степени, как и смарт-карты, но без сложностей и лишних затрат, связанных с использованием считывателя. iKey являются идеальным инструментом для контроля доступа к сетевым службам. iKey 2000 поддерживает и интегрируется со всеми основными прикладными системами, работающими по технологии PKI и используемыми в сетях отдельной организации, нескольких взаимодействующих организаций. Указанные системы включают Microsoft Internet Exolorer и Outlook, Netscape, Entrust, Baltimore, Xcert, Verisign и др. iKey 2000 разрабатывался для защиты цифровой идентичности в рамках инфраструктуры открытых ключей (PKI). iKey 2000 способен с помощью аппаратных средств генерировать и сохранять в памяти пары открытых ключей и цифровые сертификаты, а также производить цифровую подпись. Личный PKI-ключ недоступен компьютеру клиента.

iKey 2000 создает мощную систему защиты и криптографического кодирования непосредственно внутри аппаратного устройства. Для iKey 2000 пользователю поставляется программное обеспечение. Устройство содержит полный набор криптографических библиотек для броузеров Netscape и Internet Exolorer, а также для клиентов электронной почты. iKey 2000 действует одновременно как смарт-карта и считыватель, находящиеся в едином устройстве с конструктивом USB. Для активизации прикладной программы достаточно вставить iKey 2000 в USB-порт.

iKey 2000 реализует более простой метод обеспечения привилегий пользователя, чем пароли или чисто программные сертификаты. Чтобы запрограммировать ключ, администратору потребуется всего несколько минут. Потерянные ключи могут быть дезактивированы и изменены.

4.11.6. Кейс «ТЕНЬ»

Предназначен для транспортировки ноутбуков под охраной с возможностью автоматического уничтожения информации при попытке несанкционированного доступа. Имеет автономный источник питания, дистанционное управление. Монтируется в пыле-, влаго-, взрывозащищенный кейс (рис. 4.52). Также может быть использован для транспортировки жестких дисков, дискет, аудио-, видео-, стримерных кассет.

Рис. 4.52. Кейс «ТЕНЬ»

Профессиональная модель предназначается для уничтожения в любой момент информации с магнитных носителей при их транспортировке. Имеет повышенную защиту, собственное микропроцессорное управление, автономный источник резервного питания. Изготавливается только под заказ, на основании определенной клиентом комплектации.

Рекомендуется как средство защиты информации (копии, дубликаты, Backup) при ее транспортировке к месту хранения. В базовой комплектации состоит из модуля уничтожения, модуля микропроцессорного управления, модуля резервного питания на 12 ч. Монтируется в стандартный чемодан типа «дипломат». Можно перевозить до 2-х накопителей, под которые рассчитан модуль уничтожения. Активация производится нажатием потайной кнопки, радиобрелка, при попытке несанкционированного вскрытия (защита всего периметра). Питание только от автономного источника питания.

Управление и защита базовых моделей может быть усилена за счет комплектации дополнительными модулями защиты, управления и оповещения.

4.11.7. Устройство для быстрого уничтожения информации на жестких магнитных дисках «СТЕК-Н»

Назначение

Изделия «Стек-Н» (рис. 4.53) предназначены для быстрого (экстренного) стирания информации, записанной на накопителях информации на же-

стких магнитных дисках, эксплуатируемых, так и не эксплуатируемых в момент стирания.

Основные особенности изделий серии «Стек»

- предельно возможная скорость уничтожения информации;
- способность находиться во взведенном состоянии сколь угодно долго без ухудшения характеристик;
- возможность применения в дистанционно управляемых системах с автономным электропитанием;
- отсутствие движущихся частей;
- стирание информации, записанной на магнитном носителе, происходит без его физического разрушения, но после стирания использование НЖМД вновь проблематично.

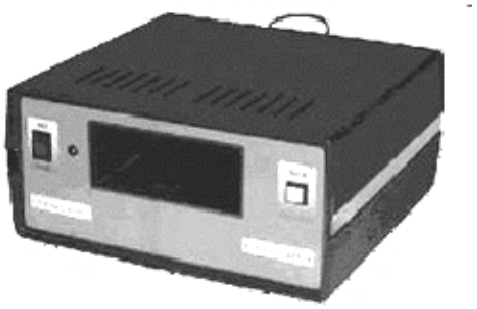


Рис. 4.53. Устройство «СТЕК-Н»

Основные отличительные особенности базовых моделей устройства «Стек-Н»

1. Модель «Стек-НС1» ориентирована на создание рабочего места для быстрого стирания информации с большого количества винчестеров перед их утилизацией. Имеет только сетевое электропитание, характеризуется малым временем перехода в режим «Готовность» после очередного стирания. Модель имеет невысокую стоимость и предельно проста в управлении.

2. Модель «Стек-НС2» ориентирована на создание стационарных информационных сейфов для компьютерных данных, имеет только сетевое электропитание. Модель оборудована системами поддержания температурного режима НЖМД, самотестирования, а также может быть дооборудована модулем дистанционной инициализации.

3. Модель «Стек-НА1» ориентирована на создание портативных информационных сейфов для компьютерных данных, имеет сетевое и автономное электропитание. Модель оборудована системой самотестирования и модулем дистанционной инициализации.

Вопросы для самопроверки

1. За счет чего можно ослабить паразитные связи?
2. В чем заключается сущность электромагнитного экранирования?
3. Как оценивается эффективность экранирования?
4. Назовите способ снижения паразитной емкости между электрическими цепями.
5. Какие виды экранирования применяют для снижения величины магнитных полей?
6. На каком принципе основано магнитостатическое экранирование?

7. В чем заключается сущность динамического экранирования?

8. Какого типа информационные линии связи обеспечивают наилучшую защиту как от электрического, так и от магнитного полей?

9. Назовите эффективный метод подавления синфазных помех в линии.

10. Что представляют собой экранированные камеры? Их назначение.

11. Что представляет собой полностью безэховая экранированная камера?

12. Какие существуют типы заземлений?

13. С какой целью применяется фильтрация сигналов?

14. Какие устройства используются для фильтрации сигналов в цепях питания ТСПИ?

15. Как подраздеделяют фильтры в зависимости от типов элементов, из которых они составлены?

16. Количественная величина ослабления фильтра.

17. Как определяется частота среза на логарифмической амплитудно-частотной характеристике фильтра?

18. В каких границах находится полоса пропускания фильтра низкой частоты?

19. В каких границах находится полоса пропускания фильтра высокой частоты?

20. В каких границах находится полоса пропускания полосно-пропускающего фильтра?

21. Какого типа помехи обеспечивают системы пространственного зашумления?

22. В каких случаях применяются системы линейного зашумления?

23. Какие технические способы применяются для исключения возможностей перехвата информации за счет ПЭМИН ПК?

24. Методы активной маскировки.

25. Поясните сущность энергетической и неэнергетической маскировок.

26. Функции электросиловых сетей как каналов утечки информации.

27. Каким образом могут использоваться телефонные линии в каналах утечки информации?

28. Функции анализатора линий.

29. В каких режимах обследуются схемы силовых и телефонных линий?

30. Основные технические возможности анализаторов линий.

31. В каких случаях применяют активные средства защиты речевой информации?

32. Что представляют собой активные средства защиты речевой информации?

33. Назовите наиболее эффективный способ защиты телефонных каналов связи.

34. Перечислите известные Вам программно-аппаратные средства защиты компьютерной информации от несанкционированного доступа.

35. Перечислите функции программно-аппаратного комплекса Secret Net 5.0.

36. Назовите состав устройства ввода идентификационных признаков на базе идентификаторов Proximity.

37. Перечислите основные узлы смарт-карты.

5. МЕТОДЫ И СРЕДСТВА ИНЖЕНЕРНОЙ ЗАЩИТЫ И ТЕХНИЧЕСКОЙ ОХРАНЫ ОБЪЕКТОВ

5.1. Категории объектов защиты

По степени важности, а, следовательно, и необходимой надежности охраны объекты принято разделять на категории, например: особо важные (ОВ), важные, общего назначения и т.п. [11].

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

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

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

5.2. Особенности задач охраны различных типов объектов

В случае несанкционированного проникновения злоумышленников на 0В наиболее вероятны диверсионные акты, направленные на уничтожение объекта, нарушение его нормального функционирования, а также действия, связанные с хищением ядерных материалов, оружия, секретной информации. Величина ущерба может возрастать со временем (например, увеличение числа пораженных лиц в результате взрыва на ядерно-опасном объекте).

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

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

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

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

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

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

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

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

Основные задачи, решаемые физическими средствами:

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

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

В самых общих чертах структура системы обеспечения безопасности объектов может содержать элементы и системы, показанные на рис. 5.1. В конкретных случаях в зависимости от специфики объектов какие-то элементы структурной схемы могут отсутствовать, а какие-то другие – присутствовать. Совершенно очевидно, что требования к безопасности объектов ОВ резко отличаются от таковых для объектов других категорий.

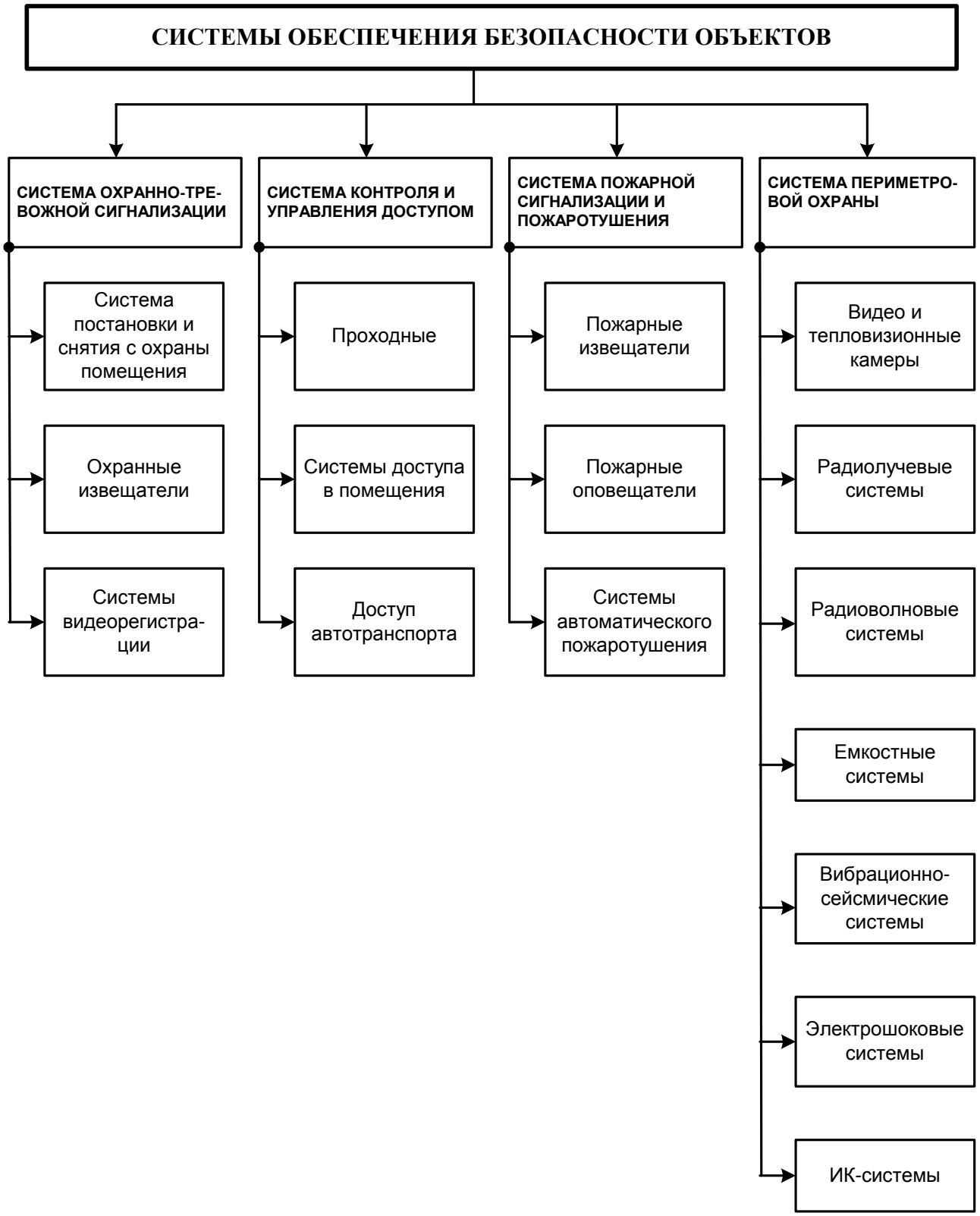


Рис. 5.1. Структура системы обеспечения безопасности объектов

Более подробное описание элементов структуры приводится в последующем тексте.

5.3. Общие принципы обеспечения безопасности объектов

В общем случае обеспечение безопасности объекта базируется на двух принципах:

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

Адекватные меры защиты предусматривают:

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

Рассмотрим особенности организации систем обеспечения безопасности объектов на примере интегрированной системы на базе прибора приемно-контрольного охранно-пожарного (ППКОП) «Рубеж-08» (рис. 5.2) [65].

Рис. 5.2. Центральный процессорный блок прибора «Рубеж-08»

Прибор служит основой для создания интегрированных систем комплексной безопасности средних и крупных объектов, в состав которых входят подсистемы: охранной сигнализации, тревожной сигнализации, пожарной сигнализации, технологической сигнализации, контроля и управления доступом, управления исполнительными устройствами и др.

5.4. Система охранно-тревожной сигнализации

Система охранно-тревожной сигнализации (ОТС) предназначена для постановки и снятия с охраны помещений; формирования и выдачи сигналов тревоги при несанкционированном появлении или попытке проникновения человека в закрытые и сданные под охрану помещения; просмотра состояния охраняемых помещений на планах в графической форме на автоматизированных рабочих местах (АРМ) интегрированной системы безопасности (ИСБ) и отображения на них сигналов тревоги или неисправности в графическом, текстовом и голосовом виде с привязкой к плану объекта; ведение протокола событий системы ОТС в памяти компьютера с возможностью просмотра на мониторе и его распечатки; ведение электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях.

Система охранно-тревожной сигнализации (ОТС) обеспечивает:

• интеграцию с другими системами ИСБ на программно-аппаратном уровне;

• ручное (аппаратное) управление постановкой/снятием с охраны с помощью электронных карт-пропусков;

• контроль состояния системы с центрального пульта, мониторов АРМ постов охраны, и других АРМов в соответствии с регламентом;

• паролирование и иерархическое распределение доступа сотрудников к функциям и регламентам системы;

• работоспособное состояние при прекращении электроснабжения – в течение не менее 4 часов;

• возможность независимой работы в случае нарушения связи с сервером или выхода из строя компьютерной техники;

Размещение оборудования системы ОТС. ППКОП «Рубеж-08» устанавливаются в помещении с постоянным присутствием людей (диспетчерская, комната мастера смены и т.п.).

Сетевые контроллеры шлейфов сигнализации, каждый из которых предназначен для подключения 16 шлейфов охранной сигнализации, устанавливаются в центральный или периферийные распределительные шкафы до 10 линейных блоков в один крейт R3 (рис. 5.3).

В качестве коммутационных коробок при построении линейной части системы ОТС используются коробки JB-20 и JB-701 имеющие 8 и 5 соединительных клемм (рис. 5.4). Данные коробки имеют достаточно свободного места для установки оконечных элементов шлейфа и небольшого запаса кабеля, для проведения нескольких перекоммутаций, а также имеют тамперные контакты, защищающие коробку от несанкционированного вскрытия.

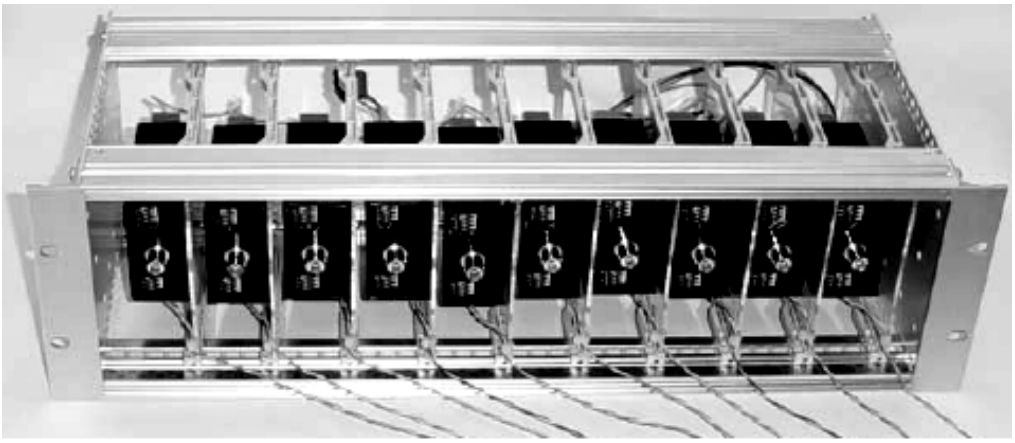


Рис. 5.3. Крейт R3

Система охранной сигнализации легко уязвима в рабочее время, когда помещения сняты с охраны и может быть подвержена постороннему вмешательству, выраженному в шунтировании шлейфов сигнализации как в коробках, так и непосредственно в охранных датчиках. Для защиты проводки системы охранной сигнализации от несанкционированного вмешательства злоумышленников применяются распределительные шкафы и разводные коробки с тамперами, которые объединяются вместе с тамперами охранных датчиков в отдельные шлейфы, находящиеся под круглосуточной охраной.

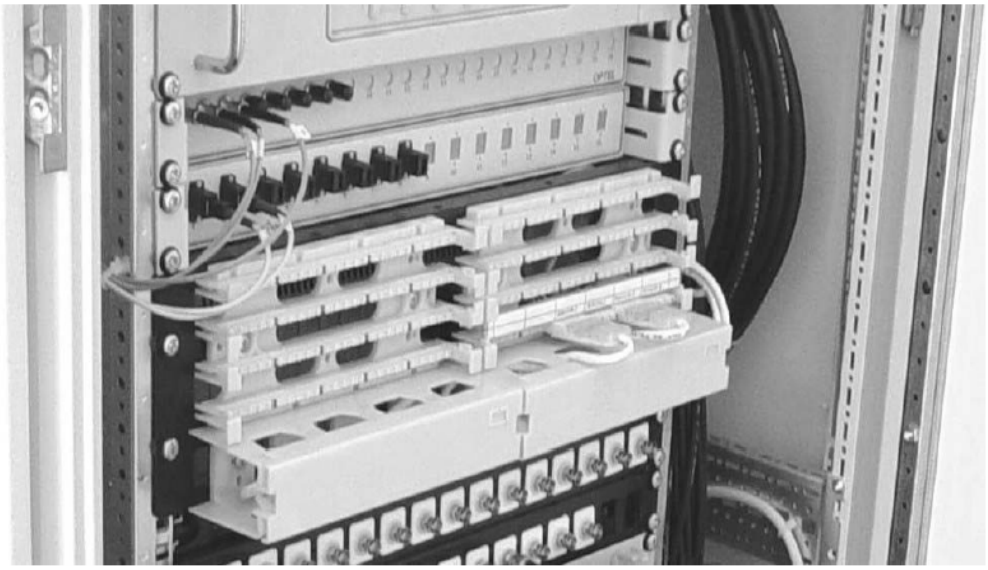


Рис. 5.4. Кабельная коробка

Применение ППКОП «Рубеж-08», который имеет возможность передачи в порт сообщений об изменении состояния каждого шлейфа (готов, не готов), совместно с программным обеспечением Security Wizard позволяет отслеживать исправность шлейфов сигнализации, при помощи отчета по проверке активности шлейфов сигнализации. При выполнении отчета зада-

ется временной параметр, например неделя. Результатом отчета будет список шлейфов, которые не изменяли своего состояния из готовности в неготовность или обратно в течение недели.

При помощи данного отчета также можно отслеживать попытки вывода из строя объемных датчиков движения при помощи аэрозоля и других средств. Для этого объемные датчики и датчики открытия дверей должны быть подключены на отдельные шлейфы сигнализации.

ППКОП «Рубеж-08» имеет в своем составе блок индикации состояний БИС-01 (рис. 5.5), предназначенный для индикации состояния объектов системы охранной сигнализации на встроенном светодиодном табло.

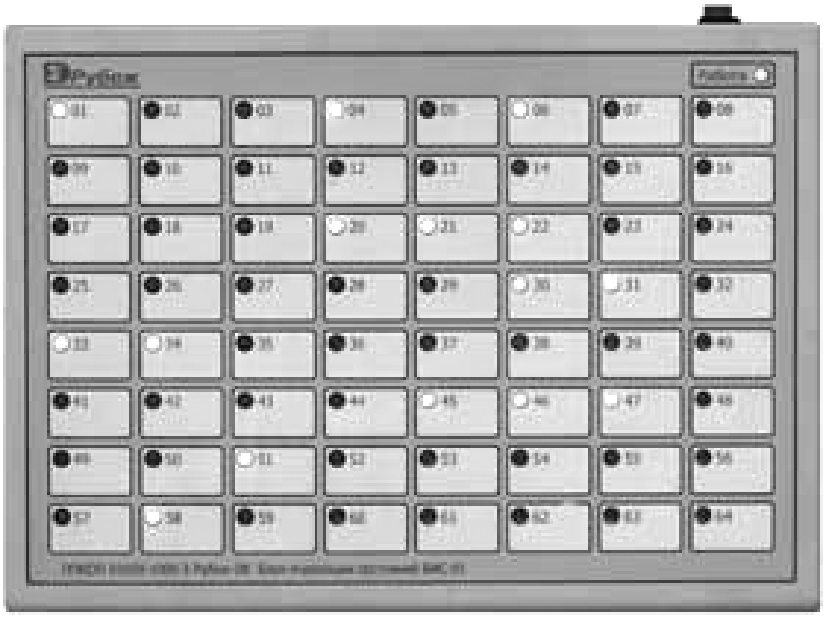


Рис. 5.5. Блок индикации состояний БИС-01

ППКОП «Рубеж-08» имеет порт RS-232 для обмена оперативной информацией с системой сбора и обработки информации, а также для обеспечения возможности управления по событиям, произошедшим в других системах, входящих в ИСБ, или по запросу оператора службы безопасности.

Система ОТС помещений. Помещения защищаются в два рубежа охраны. Для однозначной расшифровки сигнала тревоги и выдачи адресного сообщения на АРМы ИСБ каждое помещение защищается отдельными зонами охранной сигнализации.

Элементы оконных проемов здания заблокированы на открытие магнитоконтактными извещателями. Дополнительно оконные проемы первого этажа, а также вышележащих этажей здания, которые выходят или примыкают к пожарным лестницам и другим строительным элементам, по которым возможно проникновение в данные помещения, заблокированы на разрушение стекла звуковыми извещателями ИО329-4 «Стекло-3». Перечисленные извещатели входят в 1 рубеж охраны.

Двери блокируются на открывание врезными магнитоконтактными извещателями. Внутренний объем помещений контролируется объемными оптико-электронными извещателями ИО409-8 «Фотон-9». Перечисленные извещатели входят во 2 рубеж охраны.

Управление постановкой/снятием с охраны помещений может осуществляться, как централизованно, так и децентрализованно. При этом все операции, связанные с управлением системой, являются персонифицированными (автоматически протоколируются с указанием ФИО пользователя и времени с точностью до секунды).

Терминал управления охранной сигнализацией состоит из блока индикации состояний БИС-01 и считывателя с кодонаборной панелью. Считыватель отвечает за постановку и снятие с охраны.

Каждой карте доступа назначается номер зоны (помещения) которую разрешено ставить и снимать с охраны по этой карте. Постановка/снятие осуществляется путем регистрации карты на считывателе терминала управления охранной сигнализацией, каждая последующая регистрация карты изменяет состояние соответствующей зоны (кабинета), при этом меняется цвет свечения светодиода БИС-01, соответствующего данному кабинету.

Для осуществления возможности сотрудникам производить постановку/снятие с охраны произвольных помещений (помимо присвоенного карте доступа), в терминале управления используется считыватель с кодонаборной панелью.

На рис. 5.6 показан пульт управления объектовый ПУО-02, который предназначен для организации объектового управления охранной сигнализацией на уровне зон ППКОП «Рубеж-08»: постановка на охрану, снятие с охраны, просмотр состояния. ПУО-02 имеет встроенную клавиатуру для ввода пинкода и команд пользователя и жидкокристаллический однострочный 16-символьный дисплей с подсветкой для отображения информации.

Для постановки под охрану пользователь набирает на клавиатуре считывателя номер операции #1 (постановка под охрану), затем номер помещения согласно экспликации помещений и регистрирует на считывателе личную электронную карту-пропуск. Снятие с охраны осуществляется аналогично, номер операции снятия с охраны #2.

Рис. 5.6. Пульт управления объектовый ПУО-02

Охранные извещатели

Охранные извещатели – это датчики системы охранной сигнализации, которые призваны обнаружить злоумышленника в охраняемом объекте, сформировать сигнал тревоги и передать его в охранную систему для принятия мер реагирования.

По физическому принципу действия извещатели можно подразделить на следующие группы [43].

Инфракрасные – извещатели, которые обнаруживают тепловое (инфракрасное) излучение человеческого тела и формируют сигнал тревоги в случае, когда источник теплового излучения движется.

Ультразвуковые – извещатели, излучающие ультразвуковые колебания и принимающие сигнал, отраженный от окружающих предметов. Формирование тревожного сигнала происходит в случае возникновения движения в контролируемой зоне.

Радиоволновые – извещатели, излучающие в диапазоне ультракоротких радиоволн. Их принцип работы аналогичен принципу работы ультразвуковых извещателей.

Барометрические – извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.

Акустические – извещатели, формирующие сигнал тревоги при регистрации в охраняемой зоне характерного звука, например, звука разбивания оконного стекла.

Сейсмические – извещатели, устанавливаемые на жесткую конструкцию и формирующие сигнал тревоги в случае регистрации в этой конструкции колебаний, возникающих при попытке разрушения преграды.

Инерционные – извещатели, в которых сигнал тревоги формируется при механическом воздействии на охраняемый объект, например автомобиль (покачивание, толчки). К группе инерционных относятся вибрационные и ударноконтактные извещатели.

Пьезоэлектрические – различные извещатели, использующие в своей работе пьезоэлектрические материалы, которые обладают свойством наведения разности потенциалов на противоположных сторонах пьезоэлектрического кристалла при его деформации. К пьезоэлектрическим относятся контактные извещатели контроля разбития стекла, извещатели контроля неподвижности установленных или подвешенных предметов и т.д.

Магнитоконтактные – извещатели, формирующие сигнал тревоги при размыкании геркона вследствие удаления от него магнитного элемента. Устанавливаются как правило на окна и входные двери.

Электроконтактные – извещатели, которые формируют сигнал тревоги при размыкании электрического контакта. В настоящее время используются как правило в системах тревожной сигнализации и работают в ручном режиме.

Комбинированные – извещатели, которые сочетают в себе два или более физических принципа действия (инфракрасный и ультразвуковой, инфракрасный и радиоволновой).

Действие извещателей основано на использовании различных физических принципов. Можно выделить два основных типа извещателей [43]:

1. Пассивные извещатели, которые сами не являются источниками волн различной физической природы (электромагнитных, акустических, пр.).

2. Активные извещатели, являющиеся источниками таких волн.

Очевидные преимущества пассивных извещателей – это их экологическая чистота и низкое энергопотребление.

Пассивные инфракрасные извещатели наиболее широко применяются для охраны помещений. Они обнаруживают тепловое (инфракрасное) излучение человеческого тела в пределах зоны чувствительности и формируют сигнал тревоги в случае, когда источник теплового излучения движется со скоростью 0,1…1,5 м/сек. Инфракрасный извещатель не регистрирует неподвижные объекты, даже если их температура превышает уровень фона (неподвижный человек) или если объект с температурой, отличной от фона, перемещается таким образом, что не пересекает чувствительных зон извещателя (например перемещается вдоль чувствительной зоны).

Тепловое излучение человеческого тела находится в пределах спектрального диапазона электромагнитного излучения с длинами волн 8…12 микрометров. Это так называемое равновесное свечение человеческого тела, максимум длины излучения которого полностью определяется температурой и для 37 °С соответствует приблизительно 10 микрометрам.

В пассивных инфракрасных извещателях используется чувствительный элемент с оптимальным соотношением чувствительность/стоимость. Таким чувствительным элементом является пироэлектрический фотоэлемент. Явление пироэлектричества состоит в возникновении наведенной разности потенциалов на противоположных сторонах пироэлектрического кристалла при его неравновесном кратковременном нагревании. Со временем электрические заряды из внешних электрических цепей и перераспределение зарядов внутри кристалла приводят к релаксации наведенного потенциала. Поэтому для эффективной пироэлектрической регистрации теплового излучения необходимо применять прерыватель с оптимальной частотой прерывания излучения около 0,1 Гц.

Для повышения термостабильности работы извещателя и исключения влияния медленно меняющейся температуры окружающей среды чувствительный элемент изготавливается в виде парной конструкции электрически встречно включенных элементов, расположенных на общей подложке. Высокая чувствительность инфракрасного извещателя достигается путем применения линзовой системы концентрации входящего излучения.

На рис. 5.7 показана одна из моделей пассивного инфракрасного извещателя – извещатель «Рапид-3», который обеспечивает:

- сверхнизкое токопотребление в режиме «норма» – 70 мкА;
- питание по шлейфу сигнализации;
- возможность подключения к шлейфу сигнализации большого числа извещателей без дополнительного подбора оконечного резистора;
- защиту от несакционированного доступа;
- четыре вида извещений: «включение», «норма», «тревога», «вскрытие».

Рис. 5.7. Инфракрасный пассивный извещатель «Рапид-3»

Автоматизированные рабочие места (АРМ) системы ОТС.

Экран АРМа может быть разделен на несколько зон:

1. Зона планировок.

Зона планировок представляет собой поле, на которое выводятся подробные планы этажей здания с нанесенными на них изображениями технических средств различных систем безопасности. Настройка отображения технических средств различных систем производится для каждого рабочего места отдельно.

В зоне планировок также размещены пиктограммы телевизионных камер. Клик мышью на иконку приводит к выводу изображения с этой телевизионной камеры на дежурный видеомонитор.

Для предотвращения засорения планов значками датчиков и отвлечения оператора, датчики, находящиеся в дежурном режиме или режиме охраны, на плане могут не отображаться. В этом режиме отображаются на плане только те датчики, на которые следует обратить внимание оператора, к примеру, датчики, находящиеся в режиме тревоги, неисправности или исключенные во время постановки под охрану.

Программное обеспечение SW позволяет подсвечивать не только пиктограммы, но и различные объекты (ломаные линии, различные фигуры и т.д.), в том числе элементы плана. Это позволяет при постановке под охрану наглядно выделять цветом на плане поставленное под охрану помещение, указывать на плане протяженную зону обнаружения технических средств с повторением изгибов ограждения, что важно при реализации инженерно-технической системы защиты периметра.

2. Журнал регистрации событий.

На терминале АРМа также размещается журнал регистрации событий, в который записываются все события, произошедшие в системе. Тревож-

ные события в журнал записываются шрифтом красного цвета. При двойном клике на интересующей строчке повторно показывается на плане датчик, находившийся в состоянии тревоги.

Взаимодействие системы ОТС с другими системами ИСБ.

По тревогам системы ОТС различные системы, входящие в ИСБ, могут быть настроены на отработку следующих алгоритмов взаимодействия:

1. При поступлении тревоги от системы ОТС может блокироваться автоматический проход через двери помещений (все или выборочно), для предотвращения доступа злоумышленников в эти помещения.

2. При поступлении тревоги из зоны с ограниченным доступом могут блокироваться выходы из этой зоны (при условии, что выход оборудован считывателем карт).

3. При поступлении тревоги от системы ОТС на тревожные мониторы системы СТН выводится изображение от видеокамеры (или изображения от нескольких камер в различных мультиэкранных режимах), в зоне ответственности которой произошла тревога.

4. При поступлении тревоги от системы ОТС управляемые камеры системы СТН могут быть выставлены в заранее запомненные позиции.

5. При поступлении тревоги от системы ОТС оборудование видеорегистрации переводится в режим записи с повышенным качеством на предварительно установленное время или на время действия тревоги.

При поступлении первой тревоги на тревожные мониторы в автоматическом режиме выводится изображение от тревожной телевизионной камеры.

Если следующая тревога возникает до того, как первая исчезла из списка тревог, то она появляется в списке тревог следующей строчкой. Последующие тревоги также выстраиваются в очередь в списке тревожных событий. Это сделано для того, чтобы дать возможность оператору перемещаться между произошедшими тревогами и реагировать в первую очередь на наиболее важные события.

Каждая следующая пришедшая тревога добавляет на тревожном мониторе изображение от камеры, в поле зрения которой произошла тревога. В свою очередь изображения, выведенные по тревогам с истекшим временем жизни, исчезают с экрана тревожного монитора, при этом в автоматическом режиме производится переключение наиболее оптимальных мультиэкранных режимов.

5.5. Система контроля и управления доступом

Функциональная организация СКУД

Система контроля и управления доступом (СКУД) предназначена для выполнения комплекса мероприятий, направленных на ограничение и санкционирование доступа сотрудников на территорию предприятия, в по-

мещения и зоны ограниченного доступа. Оборудование рассчитано на количество пользователей системы контроля и управления доступом электронной проходной до 65 000 человек и до 5 000 человек для выделенных помещений.

СКУД обеспечивает:

• интеграцию с другими системами ИСБ на программно-аппаратном уровне;

• многоуровневую организацию доступа с возможностью корректировки базы данных администратором ИСБ в соответствии с решаемыми задачами;

• возможность графического отображения состояния u1089 системы (наличие тревог, нештатных ситуаций, оперативной информации с выводом поэтажных планов, мест установки технических средств системы КУД);

• создание архива с объемом памяти, обеспечивающим регистрацию всех фактов посещения предприятия сотрудниками и посетителями с указанием даты и времени посещения, их фотографий и иных данных с возможностью хранения и использования в течение одного года;

• возможность ежедневного архивирования базы данных разовых посетителей в конце рабочего дня, ведение протоколов, электронных журналов;

• возможность перехода на ручное управление отдельными элементами СКУД с защитой паролем и подтверждением дежурным службы безопасности с автоматическим протоколированием данного факта;

• возможность развития за счет расширения программно-аппаратных частей без нарушения работоспособности смонтированного оборудования, а также возможность модернизации в случае изменения или расширения функций (задач), выполняемых системой.

Электронная проходная сотрудников и посетителей

СКУД электронной проходной обеспечивает:

• санкционированный доступ (вход и выход) сотрудников на территорию предприятия (основанием санкционированного доступа является карта-пропуск);

• вывод фотоизображения сотрудников, имеющих постоянные и временные пропуска на мониторе оператора поста охраны на КПП;

• возможность блокирования выхода через проходные в случае поступления сигнала тревоги;

• компьютерный учет входа и выхода посетителей и сотрудников с ведением протокола в компьютере и выводом протокола на принтер.

Центральная проходная может быть оборудована электромеханическими турникетами типа «трипод» (рис. 5.8). С обоих сторон турникета устанавливаются считыватели для регистрации и контроля работников предприятия. Управление проходами через турникеты может осуществляться

как в автоматическом, так и в полуавтоматическом (с принятием решений вахтером) и ручном режимах. Выбор режима осуществляется на программном уровне.

Рис. 5.8. Электромеханические турникеты типа «трипод»

Рабочее место вахтера оборудуется АРМом с ПО SW по одному для каждого прохода.

На АРМах может быть реализован режим фотоидентификации, время вывода фотографии находится в районе 1с. Для ручного управления турникетами на рабочем месте устанавливаются специальные кнопочные панели.

Доступ в зоны, выделенные помещения и кабинеты

СКУД обеспечивает:

• санкционированный доступ сотрудников в зоны, выделенные помещения и кабинеты согласно разграничению прав доступа;

• выдачу сигнала тревоги на АРМ СКУД в случае несанкционированного проникновения в зоны доступа и выделенные помещения (вскрытие двери) или в случае не закрытия двери;

• блокирование выхода из зоны в случае поступления сигнала тревоги или при попытке несанкционированного прохода;

• компьютерный учет входа и выхода посетителей и сотрудников с ведением протокола в компьютере и выводом протокола на принтер;

• контроль и регистрацию перемещения сотрудников в протоколе компьютера;

• аварийную разблокировку дверей с поста охраны центрального входа.

Для санкционированного доступа сотрудников в кабинеты на вход и на выход могут применяться автономные контроллеры доступа (считыватели), часть из которых представлена ниже.

Автономный контроллер доступа на 1 точку прохода представлен на рис. 5.9. Контроллер интегрирован в единый корпус с proximity считывателем. Память устройства 2044 карт, дальность чтения карты 10 см, трехцветный светодиод, зуммер, размер 90×50×18 мм, рабочий диапозон от –40 до +50 °С. Программирование мастер картой

Работа с ПК не поддерживается. Возможно подключение к контроллеру дополнительного бесконтактного считывателя EM-Reader.

Производитель: Prox.

Proximity (проксимити) считыватель EM-Reader-ME, в антивандальном корпусе, для СКУД формата EM-marin, дальность 4-6 см, размеры 70х50х20мм, 8..15В/ 30мА, от – 40 до +50С, выход: Weigand 26,34,37,40,42, эмуляция DS1990A (рис. 5.10).

Производитель: Prox.

Биометрический контроллер (считыватель по отпечатку пальца) (рис. 5.11), кодонаборная панель, дисплей, программируется с помощью клавиатуры или ПО (в комплекте) по RS232, память – 1920 пользователей, буфер – 8190 событий, интерфейс Wiegand, RS232 (опции RS 422, PCP/ IP) Производитель: Keico

Рис. 5.9. Автономный контроллер доступа Em-contr

Рис. 5.10. Считыватель EM-Reader-ME

Рис. 5.11. Биометрическая система EPC-311PF/B+IDC

Биометрический контроллер (рис. 5.12) содержит считыватель по отпечатку пальца, кодонаборную панель, встроенный Prox-считыватель. Программируется с помощью клавиатуры или ПО (в комплекте) по RS232 (память – 4480 пользователей, буфер – 8190 событий).

Производитель: Keico.

Рис. 5.12. Биометрический контроллер KF-1000PFC/C

Доступ автомобильного транспорта на территорию объекта через КПП

СКУД обеспечивает:

- санкционированный доступ автотранспорта на территорию предприятия (основанием для доступа сотрудников и автотранспорта на территорию предприятия является электронная карта-пропуск);
- контроль обстановки в зоне досмотра автотранспорта, а также обзор государственного регистрационного номера транспортного средства из помещения поста охраны КПП средствами телевизионной системы наблюдения.

Снаружи каждого КПП устанавливается шлагбаум. Для дистанционного управления шлагбаумом на КПП устанавливается наружный пульт охраны.

Взаимодействие СКУД с другими системами ИСБ

По различным тревогам системы, интегрированные в комплекс ИСБ, могут быть настроены на отработку различных алгоритмов взаимодействия.

Автоматизированное управление СКУД по сигналам от других систем

От системы ОТС

1. При поступлении тревоги от системы ОТС может блокироваться автоматический проход в оба направления через двери по постоянным и временным пропускам.

2. При поступлении тревоги из зоны с ограниченным доступом могут блокироваться выходы из этой зоны (при условии, что выход оборудован считывателем карт).

От системы пожарной сигнализации

При поступлении сигнала «пожар» возможен вывод меню автоматической команды, имеющей, например, следующие кнопки:

- Разблокировать двери кабинетов.
- Разблокировать все точки доступа.
- Отмена.

Меню команд имеет задержку, необходимую для возможности оценки дежурным степени угрозы с целью принятия верного решения. В случае непринятия решения в течение установленного времени запрограммированное действие запустится автоматически.

Автоматизированное управление другими системами по тревогам СКУД

1. При поступлении сигнала «взлом двери» от системы КУД на тревожные мониторы СТН выводится изображение с видеокамеры, установленной в коридоре, в который выходит взломанная дверь, а оборудование видеорегистрации переводится в тревожный режим записи.

2. При поступлении сигнала о не закрытии двери от системы КУД на тревожные мониторы СТН выводится изображение с видеокамеры, установленной в коридоре, в который выходит взломанная дверь.

5.6. Телевизионные системы

Телевизионные системы широко применяются для наблюдения за территорией охраняемого объекта или за обстановкой внутри помещения. Практически такие системы имеют общую структуру: несколько передающих ТВ-камер подключаются к центральному пульту, где устанавливаются один или несколько мониторов, на которые можно выводить изображение от любой из передающих камер. При сходной структуре различные системы отличаются типами используемых ТВ-камер и схемой подключения к центральному пульту. Особенности работы системы телевизионного наблюдения (СТН) кратко рассмотрим на примере системы «Интеллект» производства компании «ЭлКом-Инжиниринг», которая по функциональным характеристикам относится к системе с расширенными функциями по ГОСТ Р 51558-2000.

СТН предназначена для:

- усиления охраны и внутриобъектового режима на охраняемом объекте;
- организации технологического наблюдения в местах установки системы пожаротушения.

СТН обеспечивает:

- интеграцию с другими системами ИСБ на программно-аппаратном уровне;
- визуальный контроль периметра предприятия, контроль выполнения технологических процессов внутри помещений объекта, контроль зоны досмотра транспортных средств, контроль государственных номеров автотранспорта, подъезжающего к внешним воротам транспортных КПП;
- получение должностными лицами дежурного персонала службы безопасности видеоинформации с телевизионных камер в соответствии с настройками системы;
- получение должностными лицами дежурного персонала производственных подразделений объекта видеоинформации с телевизионных камер;
- приоритетное включение каналов для просмотра и запись при срабатывании технических средств систем безопасности в зоне наблюдения телекамер;
- круглосуточную запись изображений со всех видеокамер с последующей возможностью воспроизведения;
- работоспособное состояние при прекращении электроснабжения в течение не менее 1 ч.

При разработке СТН учитываются следующие основные требования:

- возможность создания единой системы видеонаблюдения со сквозной нумерацией всех камер и единой базой данных о конфигурации системы;
- возможность интеграции СТН в комплекс инженерно-технических средств охраны;

- возможность расширения общего количества видеокамер;
- наличие на АРМ постов охраны тревожных телевизионных мониторов, вывод изображений на которые возможен в автоматическом режиме по сигналам от технических средств других систем, входящих в интегрированную систему безопасности (ИСБ);
- удобный графический интерфейс Windows компьютерных мониторов АРМов операторов и возможность просмотра «живого» видео (1, 4, 16, 32 камер на одном экране) и любого фрагмента из архива, а также управление камерами и параметрами записи;
- одновременный вывод на один компьютерный монитор АРМа изображения любых камер (при наличии соответствующих прав) вне зависимости от того, к какому видеосерверу они подключены;
- осуществление администрирования системы с рабочего места с соответствующими полномочиями администратора;
- наличие средств управления выводом изображений от всех видеокамер на мониторы постов наблюдения, записи (круглосуточной, по расписанию, по детектору движения, по тревогам в системах, входящих в ИСБ, по запросу оператора);
- обеспечение скорости записи не менее 7 кадров в секунду по каждой камере при максимальном качестве изображения;
- оперативное видеоархивирование в течение не менее одной недели в непрерывном режиме записи с использованием современных средств хранения информации с возможностью поиска и просмотра видеофрагментов по нескольким параметрам: дате, времени и событиям;
- возможность передачи оцифрованного видеокадра или видеосюжета по локальной сети, распечатки видеокадра на принтере, а также записи видеокадров/ видеосюжетов на CD или другие стандартные переносные носители.

Видеокамеры

Видеокамеры наблюдения могут устанавливаться стационарно и с поворотными устройствами в зависимости от специфики наблюдаемых участков. Для камер с трансфокаторными объективами целесообразно использование поворотного устройства. Использование поворотного устройства позволяет не только получить более полную «картину» всего объекта, но и производить детальный контроль нескольких объектов без значительного удорожания системы в целом.

Видеосигналы и сигналы управления от телевизионных камер, помеченных в перечне объекта как находящиеся в условиях сильных электромагнитных помех, транслируются на зональный узел по волоконно-оптической линии связи, а в остальных случаях – по кабельным линиям связи. Сигналы от остальных телевизионных камер, относящихся к системе

охранного наблюдения, транслируются по локальной вычислительной сети (ЛВС) предприятия.

В СТН могут применяться как цветные (рис. 5.13) так и черно-белые (рис. 5.14) видеокамеры. Данные видеокамеры используются в качестве базовых для организации видеонаблюдения. Черно-белые телекамеры стоят в полтора раза дешевле цветных, у них выше разрешающая способность (в полтора-два раза) и чувствительность (в 4–8 раз). Их следует применять при наблюдении больших открытых территорий. Они хорошо работают в условиях низкой освещенности, небольшого тумана.

Рис. 5.13. WV-CP480 – Высококачественная цветная камера с расширенным динамическим диапазоном

Рис. 5.14. QX-580SA – Черно-белая видеокамера

Для управляемых видеокамер, предназначенных для работы в условиях сильной запыленности, целесообразно использовать интегрированную систему позиционирования с термокожухом для сложных условий эксплуатации, например, Esprit® ES3012-5W-X производства компании Pelco (рис. 5.15).

Некоторые характеристики системы Pelco.

- Исполнение: уличное, скорость ветра до 208 км/ч, – 40° – +50 °С.
- Допускает установку любой камеры и трансфокатора (свободное пространство 88×81×307 мм).
- Оснащена двухплоскостным поворотным устройством (скорость до 100°/ с).
- Пропорциональное панорамирование.
- Кожух оснащен стеклоочистителем.

Рис. 5.15. Система позиционирования «Pelco»

Организация цифровой части СТН

Оцифровка видеосигнала, сжатие и предоставление его в компьютерную сеть благодаря встроенному Веб-серверу (Ethernet 10/100) осуществляется при помощи видеосерверов 2401+ и 2411 производства компании Axis. Видеосервер Axis 2401+ (рис. 5.16) помимо оцифровки видеосигнала позволяет передавать сигналы управления телеметрией.

Рис. 5.16. Видеосервер Axis 2401+

Видеосервер осуществляет оцифровку входящих видеосигналов, производит детекцию движения, выводит видеоизображения на свой монитор, предоставляет видео в сеть и производит запись на имеющиеся жесткие диски.

Все видеосерверы объединяются в локальную вычислительную сеть, посредством портов 10BASE-T, 100BASE-TX, или 1000BASE-T, с разъёмом RJ45 и берут данные о конфигурации с единой БД. Таким образом, создается единое пространство видеокамер со сквозной нумерацией. На каждом сервере можно просматривать любые камеры в любом сочетании.

АРМы СТН выполнены на базе компьютеров, подключенных к ЛВС предприятия, с установленными клиентскими версиями программного обеспечения, позволяющими выводить на мониторы изображения от различного числа камер в разных мультиэкранных режимах. Возможен автоматизированный просмотр записей по тревожным событиям.

Состав постов наблюдения СТН

АРМы постов наблюдения подразделяются на:

- АРМ центрального поста видеонаблюдения;
- АРМ центрального диспетчерского пульта;
- АРМ оператора службы безопасности.

АРМы СТН постов охраны состоят из компьютерных 24” LCD мониторов, на которые выводятся изображения от телевизионных камер в различных мультиэкранных режимах и специализированных мониторов для видеонаблюния.

Вывод изображений на мониторы может осуществляться как в автоматическом режиме по сигналам от технических средств интегрированных систем обеспечения безопасности, так и в ручном режиме путем воздействия манипулятора «мышь» на пиктограмму видеокамеры, размещенной на планировке объекта. Управление поворотными камерами с трансфокатором может осуществляться при помощи клавиатуры, манипулятора «мышь» или компьютерного джойстика.

Администрирование может осуществляться с любого из серверов или со специальных рабочих мест администраторов (по паролю).

Автоматическая видеозапись

ПО «Интеллект» обеспечивает цифровую видеозапись от нескольких ТВ-камер одновременно (число ТВ-камер не ограничено). Запись ведется двумя способами: вручную и автоматически – при возникновении активности в кадре. Кроме того, осуществляется автоматическая и ручная настройка любых параметров для каждой ТВ-камеры системы (продолжительности и темпа записи, приоритета обслуживания, цветности, контрастности и т.д.).

Синхронная с видео аудиозапись по одному из каналов возможна в любой момент времени (при подключении аудиоподсистемы Интеллекта).

Системой автоматически производится запись событий, предшествующих моменту обнаружения постороннего объекта в поле зрения ТВ-камер. В дальнейшем пользователь может, просматривая видеозапись, отследить, как возникла тревожная ситуация и идентифицировать объект-нарушитель.

Видеонаблюдение и детекция движений

Естественные оптические помехи (дождь, снег, плохая освещенность, качающаяся листва и трава и т.д.), неизбежно присутствующие в видеосигнале при наружной установке ТВ-камер, устраняются автоматически – за счет применения разработанных ITV интеллектуальных технологий.

ПО «Интеллект» оснащено мощным программным детектором движений, автоматически регистрирующим перемещения в охраняемой зоне. Пользователь может регулировать чувствительность детектора в зависимости от типа объектов, движущихся в поле зрения ТВ-камер (люди, животные, автомобили и т.д.). После этого система будет реагировать только на объекты заданного типа, не допуская ложных срабатываний.

Сохранение видеоданных

Благодаря применению алгоритма видеокомпрессии Delta-Wavelet, обеспечивается поддержка видеоархива большого объема (размер одного кадра варьируется в пределах от 2 до 176 Кб). «Интеллект» предоставляет широкие возможности по поддержке видеоархива. Архивные данные защищаются паролем от несанкционированного доступа.

Элементы интерфейса управления видеоархивом реализованы в виде кнопок виртуального видеомагнитофона. Помимо обычных функций (двустороннее воспроизведение, перемотка, пауза и т.д.), пользователю доступны:

- покадровый и ускоренный просмотр видео;
- цифровое масштабирование любого участка кадра;
- поиск кадров по дате, времени, номеру камеры;

• экспорт кадров в формат JPG, видеофрагментов – в AVI формат;

• печать любого кадра из архива;

• просмотр видеоархива без остановки видеозаписи и отключения детектора движения.

Программное обеспечение АРМ Интеллект

Интерфейс программного обеспечения АРМа ничем не отличается от интерфейса видеосервера и представляет собой гибко конфигурируемый на каждое рабочее место экран (группу экранов), на котором размещается нужное количество картинок от любых видеокамер системы.

Матричный коммутатор CM6800E

Матричный коммутатор предназначен для синхронизированного переключения между видеокамерами (до 48), управления видеокамерами. Внешний вид матричного системного контроллера коммутатора представлен на рис. 5.17.

Рис. 5.17. Внешний вид системного контроллера CM9760-KBD-X

5.7. Система пожарной сигнализации

Назначение системы пожарной сигнализации (ПС)

Система ПС предназначена для:

• выдачи адресного сообщение об обнаружении очага возгорания в помещение поста охраны с указанием адреса датчика (для каждого датчика в отдельности задается уровень чувствительности для выдачи сообщения «внимание» и «пожар», раздельно для дневного и ночного режимов);

• выдачи сообщение «неисправность» в помещение поста охраны с указанием адреса датчика;

• выдачи сигнала «пожар», на систему оповещения людей о пожаре, пускатели системы для блокирования приточной вентиляции и на другие системы;

• управления установками автоматического пожаротушения;

• возможности работы в автономном режиме с выполнением вышеуказанных требований;

• фиксацию факта и времени обнаружении очага возгорания, и отображение информации в реальном масштабе времени на мониторах АРМов операторов ИСБ;

• просмотра состояния охраняемых помещений на планах в графической форме на АРМах ИСБ и отображения на них сигналов «пожар» или «неисправность» в графическом, текстовом и голосовом виде с привязкой к плану объекта или его части;

• ведение протокола событий системы ПС в памяти компьютера с возможностью просмотра на мониторе и его распечатки;

• ведение электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях.

Выбор пожарных извещателей

Следует отдать предпочтение пожарной сигнализации, построенной на основе высококачественного профессионального оборудования в области систем пожарной сигнализации, например, на основе адресно-аналоговых пожарных извещателей и оповещателей компании System Sensor.

Адресно-аналоговые системы являются более высокой ступенью в развитии систем пожарной безопасности. Основным отличием от адресных и традиционных пороговых систем является то, что пожарный извещатель измеряет уровень задымленности, температуру в помещении и передает эту информацию на приёмно-контрольную панель (ППК), которая принимает решения о дальнейшем функционировании всех элементов системы в целом в соответствии с настройками. Подобное построение пожарной системы позволяет с помощью ППК учитывать различные факторы (не только степень задымления камеры датчика, либо температуру в помещении), совокупный анализ которых позволяет повысить достоверность обнаружения пожара, и как следствие – избежать остановки технологического цикла в результате ложной тревоги.

В качестве базового извещателя для большинства помещений можно применить оптико-электронный дымовой извещатель 2251ЕМ (рис. 5.18).

В основе работы оптического дымового извещателя 2251ЕМ лежит принцип рассеивания света. Он способен обнаруживать светлый дым, частицы которого достаточно велики по размеру. Используется в случае, когда сообщение о пожаре нужно получить как можно раньше, уже на этапе тления.

Рис. 5.18. Оптико-электронный дымовой извещатель 2251ЕМ

В кабельных туннелях и трансформаторных подстанциях, учитывая специфику газовыделения при горении кабельной продукции, а так же вы-

сокую запыленность указанных помещений в особенности кабельных тунелей, целесообразно использовать дымовые ионизационные пожарные извещатели 1251Е.

Данные извещатели используют слабый источник радиоактивности для ионизации молекул воздуха в чувствительной камере. Генерируемые ионы переносят электрические заряды, создавая в измерительной цепи небольшой электрический ток, значение которого уменьшается при проникновении в камеру частиц дыма.

Извещатель отличается:

• высокой чувствительностью, что обеспечивает раннее обнаружение дыма;

• отсутствием влияния запыления дымовой камеры на чувствительность извещателя;

• отсутствием зависимости чувствительности извещателя от «цвета» дыма.

В извещателях 1251Е используется источник радиоактивности в 100 раз меньше порога мощности, с которого изделия подлежат контролю и учету, в связи с чем данные извещатели не подлежат контролю и учету (подтверждено документально), а как следствие – к данным извещателям не предъявляются особые требования к утилизации.

В газораспределительных пуктах, категория зданий которых по пожароопасности относится к группе А и является взрывопожароопасной, целесообразно примененять искробезопасные извещатели 2251EIS (рис. 5.19).

Оборудование, установленное во взрывоопасной зоне, должно иметь искробезопасное исполнение, его эксплуатация не должна быть причиной возникновения взрывоопасной ситуации. Соблюдение требований по допустимым емкости и индуктивности шлейфа, обеспечивает при его обрыве или коротком замыкании отсутствие искры, а, следовательно, и его искробезопасность.

Рис. 5.19. Искробезопасный извещатель 2251EIS

Технические характеристики 2251EIS соответствуют характеристикам 2251EM.

Пожарные оповещатели

Пожарные оповещатели подразделяются на следующие:

• световые оповещатели;

• звуковые оповещатели.

В качестве звуковых оповещателей возможно применение адресно-аналоговых оповещателей EMA24ALR (рис. 5.20).

Рис. 5.20. Звуковой оповещатель EMA24ALR

Звуковые оповещатели EMA24ALR являются адресно-аналоговыми и их питание осуществляется от адресного шлейфа. Уровень звукового сигнала на расстоянии 3 м от оповещателя 87 дБ, что значительно превышает требования НПБ 104-03 (по п.3.14 – не менее 75 дБ на расстоянии 3 м от оповещателя). Уровень звукового сигнала на расстоянии 1 м от оповещателя 97 дБ. Встроенный потенциометр позволяет при необходимости ослабить звук на 0–15 дБ и уменьшить ток потребления. Стандартный EMA24ALR формирует 16×2 типов различных сигналов, выбор которых производится при помощи 4-х микропереключателей.

В качестве световых оповещателей для административных и бытовых помещений могут применяться световые табло «Блик-С-12», а для производственных помещений и цехов – световые оповещатели «Сова-К».

Структура построения системы ПС

ППКОП «Рубеж-08» размещаются, как правило, в комнатах дежурных в различных корпусах предприятия. Все ППКОП «Рубеж-08» объединяются в единую сеть посредством ЛВС предприятия.

При значительной отдаленности защищаемого помещения от ППКОП устанавливаются распределительные навесные шкафы, в каждом из которых, размещается сетевой контроллер адресных устройств СКАУ-01 и блоки питания.

ППКОП и распределительные шкафы соединяются между собой двумя линиями связи RS-485 и линией питания.

Автоматизированные рабочие места

Для контроля системы ПС и системы автоматического пожаротушения возможна организация 1 АРМа в помещении центрального диспетчерского пульта. Дополнительно предусмотрено 9 модулей клиентского программного обеспечения, устанавливаемого на существующие компьютеры рабочих мест сотрудников из числа административного и технического персонала. Связь АРМ с сервером SW осуществляется посредством ЛВС предприятия.

Взаимодействие системы ПС с другими системами безопасности

По тревогам системы ПС различные системы интегрированной системы безопасности могут быть настроены на отработку следующих алгоритмов взаимодействия:

1. На компьютерном терминале дежурного появляется меню автоматической команды имеющей, например, следующие кнопки:

- Разблокировать двери запасных выходов.
- Разблокировать входные шлюзы и двери запасных выходов.
- Разблокировать двери кабинетов.
- Разблокировать все точки доступа.
- Отмена.

Меню команд имеет задержку, необходимую для возможности оценки дежурным степени угрозы с целью принятия верного решения. В случае непринятия решения в течение установленного времени заранее запрограммированное действие выполнится автоматически.

2. На тревожные мониторы системы СТН выводится изображение от видеокамеры (или мультиэкранные изображение от нескольких камер), в зоне ответственности которой произошла тревога.

3. Оборудование видеорегистрации переводится в тревожный режим записи на время действия сигнала тревоги.

Система автоматического пожаротушения

Системой автоматического пожаротушения оборудуются, как правило, кабельные туннели. Применяется модульная система порошкового пожаротушения. Управление системой пожаротушения производится при помощи специализированных сетевых контроллеров, входящих в состав оборудования ППКОП «Рубеж-08».

Модули порошкового пожаротушения

Модуль порошкового пожаротушения МПП-2,5 (БУРАН-2,5) предназначен для тушения и локализации пожаров твердых материалов, горючих жидкостей и электрооборудования до 5000 В в производственных, складских, бытовых и других помещениях. Модуль МПП-2,5 является основным элементом для построения автоматических установок порошкового пожаротушения импульсного типа. МПП-2,5 обладает функцией самосрабатывания.

Тушению не подлежат щелочные и щелочноземельные металлы, а также вещества, горение которых может происходить без воздуха. Модуль предназначен для тушения без участия человека загораний твердых материалов (класс пожаров А), горючих жидкостей.

5.8. Периметровая охрана

Функциональные зоны охраны

При создании периметровой охраны ОВ объекта его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон: обнаружения, наблюдения, сдерживания, поражения, в которых располагаются соответствующие технические средства [11].

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

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

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

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

Оптимизация построения периметровой охраны

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

Таким образом, при построении эффективной системы охранной безопасности (СОБ) объекта необходимо решить задачу оптимизации конфигурации и длины периметра, количества рубежей, физических барьеров (ФБ), средств нейтрализации и поражения, дислокации персонала охраны и т.п. [11].

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

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

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

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

Требования к системе периметровой охраны

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

Периметровая граница объекта является наилучшим местом для раннего обнаружения вторжения, т.к. нарушитель сталкивается прежде всего с физическим периметром и создает возмущения, которые можно зарегистрировать специальными датчиками. Если периметр представляет собой ог-

раждение в виде металлической решетки, то ее приходится перерезать или преодолевать сверху; если это стена или барьер, то через них нужно перелезть; если это стена или крыша здания, то их нужно разрушить; если это открытая территория, то ее нужно пересечь.

Все это вызывает физическое взаимодействие нарушителя с периметром, который предоставляет хорошую возможность для электронного обнаружения, т.к. нарушитель создает определенный уровень вибраций, содержащих специфический звуковой «образ» вторжения. При определенных условиях нарушитель может избежать физического контакта с периметром. В этом случае применяют «объемные» датчики вторжения, играющие роль вторичной линии защиты.

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

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

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

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

Периметровые системы используют, как правило, систему распределенных или дискретных датчиков, общая протяженность которых может

составлять несколько километров. Такая система должна обеспечивать высокую надежность при большом диапазоне изменения окружающей температуры и внешних условий (дождь, снег, сильный ветер). Поэтому любая система должна обладать свойством автоматической адаптации к погодным условиям и возможности дистанционной диагностики.

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

Периметровые средства охраны (СО) используются в тех случаях, когда [11]:

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

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

Тепловизионные системы

Современные охранные телевизионные системы широко используются на самых различных объектах, поэтому существует необходимость улучшения их тактико-технических характеристик. Сделать это можно за счет применения тепловизионной аппаратуры и интеллектуализации обработки видеосигналов путем применения цифровых технологий. В отличие от ТВ-камер на приборах с зарядовой связью (ПЗС матрицах) или ТВ-камер, сочлененных с усилителями яркости изображения, в тепловидении используется совершенно другой источник информации, недоступный невооруженному глазу человека. Это собственное излучение нагретых тел, не зависящее от уровня освещенности и времени суток. Данное излучение обрабатывается и преобразовывается в видимое изображение, а так как излучение тепловой энергии присуще всем без исключения телам, то с помощью тепловизионных приборов можно наблюдать все тела и предметы в спектральном диапазоне длин волн 3–5 и 8–14 мкм, температура которых представляет интерес для охраны объектов [11].

Спектральный диапазон действия тепловизионной аппаратуры является более благоприятным, чем видимый и ближний ИК диапазоны [12]. В этом отношении тепловизионные приборы менее уязвимы, чем и определяется их большая дальность действия, так как частицы тумана и дымки меньше рабочей длины волны этой аппаратуры.

Тепловизионные средства наблюдения за объектами ночью и днем, а также в ухудшенных условиях видимости в сравнении с традиционными приборами наблюдения обладают следующими принципиальными преимуществами:

- возможность круглосуточного наблюдения (причем в темное время суток дальность видения увеличивается);
- пассивный принцип работы;
- обнаружение следов транспортных средств;
- возможность распознавания малых объектов (человека) на фоне больших и средних, а также контроля динамики обстановки в зоне наблюдения.

Современные тепловизионные приборы позволяют обнаружить человека на расстоянии 1–5 км. Сдерживающим фактором широкого внедрения тепловизионных средств в охранных системах является их высокая стоимость. Ведущие зарубежные компании стремятся снизить стоимость за счет модульного принципа построения аппаратуры и применения матричных неохлаждаемых микроболометров.

Рис. 5.21. Уличная тепловизионная камера Pelco ES30TI

Интегрированный комплект ES30TI компании Pelco на базе тепловизора Flir (рис. 5.21) позволяет осуществлять видеонаблюдение в дальнем ИК-диапазоне спектра при любых атмосферных условиях: туман, дождь, снегопад или ночь при температурах от –45 до +50 ºС и порывах ветра до 58,1 м/с.

Блок тепловизора размещен во всепогодном корпусе со степенью защиты IP66, который установлен на скоростное поворотное устройство.

Эта тепловизионная камера использует в качестве тепловизионного приемника неохлаждаемую микроболометрическую матрицу из 320×240 элементов со спектральной чувствительностью 7,5–13,5 мкм (длинноволновая область ИК-спектра) и температурной чувствительностью 0,040°. При поглощении тепла теплочувствительными элементами матрицы изменяется электрическая проводимость полупроводниковых переходов, соединяющих теплочувствительные элементы. Электрические потенциалы обрабатываются процессором и на основе полученных данных тепловизионная камера формирует картину распределения температуры, которую и видит оператор системы видеонаблюдения на экране обычного видеомонитора.

Независимо от погодных условий тепловизионная камера позволяет выбирать различные цветовые схемы изображения, выводимого на экран оператора: черно-белую, цветную или их комбинацию. В черно-белом ре-

жиме наиболее теплые области в поле зрения камеры отображаются как белые, наиболее холодные – как черные (или наоборот). В цветном режиме теплые области выделяются красным цветом, а холодные – синим. Для удобства оператора на экран с изображением можно вывести информацию об угле азимута (горизонталь), угле места (вертикаль), о режиме работы камеры и другие параметры.

Все модели тепловизионных камер серии ES30TI подключаются к устройствам системы видеонаблюдения так же, как и любые традиционные поворотные камеры наблюдения. Видеосигнал с камеры передается на принимающее устройство (монитор или видеорегистратор) по коаксиальному кабелю.

Способность обнаруживать объекты в невидимой человеческому глазу области спектра делает тепловизионные камеры оптимальным решением для обнаружения вторжений на охраняемую территорию и позволяет построить систему видеонаблюдения объекта или его периметра полностью независимую от погодных условий и освещенности.

Инфракрасные системы

Инфракрасные пассивные элементы применяются главным образом внутри помещений и были рассмотрены ранее.

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

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

Источником помех может быть также прямая засветка приемника солнечными лучами. Чаще всего это случается на закате или рассвете, когда солнце стоит низко над горизонтом. Согласно российским стандартам датчик должен сохранять работоспособность при естественной освещенности не менее 10000 лк и не менее 500 лк – от электрических осветительных приборов. Большинство современных отечественных и зарубежных лучевых датчиков имеют специальные средства фильтрации фонового излуче-

ния и отвечают указанным выше требованиям. Однако для обеспечения высокой помехозащищенности от засветки очень важно правильно юстировать датчик при его настройке и выполнять все рекомендации изготовителя по монтажу.

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

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

Одними из распространенных отечественных ИК-лучевых охранных приборов является извещатель цифровой охранный оптико-электронный «Филин» (рис. 5.22). Извещатель предназначен для охраны периметров различных объектов.

Рис. 5.22. Извещатель цифровой охранный оптико-электронный «Филин»

Принцип действия извещателя основан на регистрации изменения уровня теплового излучения при движении людей в зоне обнаружения.

Извещатель обладает низким потреблением тока (13 мА) и узкой зоной обнаружения.

Извещатель выполнен на основе цифровой технологии, что позволяет обнаруживать медленно движущегося нарушителя (от 0,1 м/с) на расстоянии 100 м.

Извещатель сохраняет работоспособность при воздействии следующих климатических факторов:

– температуре окружающего воздуха от минус 40 °С до плюс 55 °С;

– относительной влажности воздуха до 98%, при температуре 25 °С.

Извещатель формирует извещение о тревоге при пересечении человеком зоны обзора в полный рост или согнувшись. Вероятность обнаружения нарушителя, не менее 0,98.

Извещатель охранный инфракрасный активный «МИК-02» (рис. 5.23) предназначен для охраны участков периметра различных объектов, неотапливаемых помещений и выдачи тревожного извещения путем размыкания выходных контактов исполнительного реле при пересечении зоны обнаружения нарушителем.

«МИК-02» относится к группе двухпозиционных оптических инфракрасных средств обнаружения, состоящих из пары «излучатель-приемник». Принцип действия извещателя основан на формировании в пространстве между излучателем и приемником невидимого глазом ИК-луча, прерывание которого вызывает сигнал тревоги.

Извещатель обеспечивает непрерывную круглосуточную работу и сохраняет свои характеристики при температуре окружающей среды от -40° до +65 °С и относительной влажности воздуха до 98% при температуре +35 °С.

Извещатель работоспособен и не выдает тревожного извещения при:

- воздействии осадков в виде дождя, тумана и снега;
- воздействии солнечной радиации;
- воздействии ветра со скоростью до 30 м/сек;
- воздействии вибрации (метро, железная дорога и т.п.);
- воздействии электростатического разряда по ГОСТ Р 50009-92.

Рис. 5.23. Извещатель охранный инфракрасный активный «МИК-02»

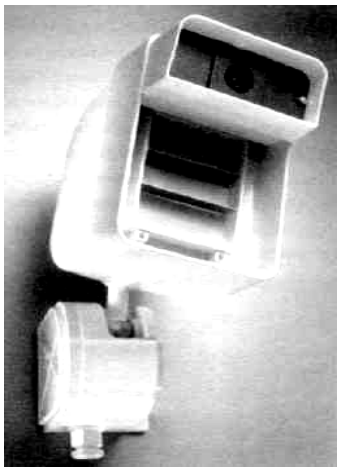


Рис. 5.24. Комбинированный ИК-датчик Redwatch-100Q с видеокамерой

Извещатель обеспечивает выдачу тревожного извещения при:

- пересечении человеком зоны обнаружения со скоростью 0,3...10 м/сек;
- одновременном пропадании напряжения сети и резервного питания;
- попытке маскирования премника извещателя;
- попытке демонтажа извещателя;
- выходе из строя блоков извещателя.

Вероятность обнаружения нарушителя – не менее 0,98.

Одна из модификаций детектора фирмы SEL – комбинированный датчик Redwatch-100Q – объединяет в себе пассивный ИК-датчик и встроенную миниатюрную видеокамеру, поле зрения которой совпадает с чувствительной зоной ИК-датчика (рис. 5.24). Возможность оперативной визуаль-

ной проверки ситуации в «тревожной» зоне сильно повышает общую эффективность охраны

Емкостные системы охраны периметров

Наиболее широко применяемыми отечественными средствами охраны периметров, использующими емкостный метод обнаружения, являются приборы серии «Радиан» [57].

Ёмкостное средство обнаружения «Радиан-14» (рис. 5.25) предназначено для охраны периметра объектов, включая ворота, с использованием в качестве чувствительного элемента сигнализационного заграждения (СЗ).

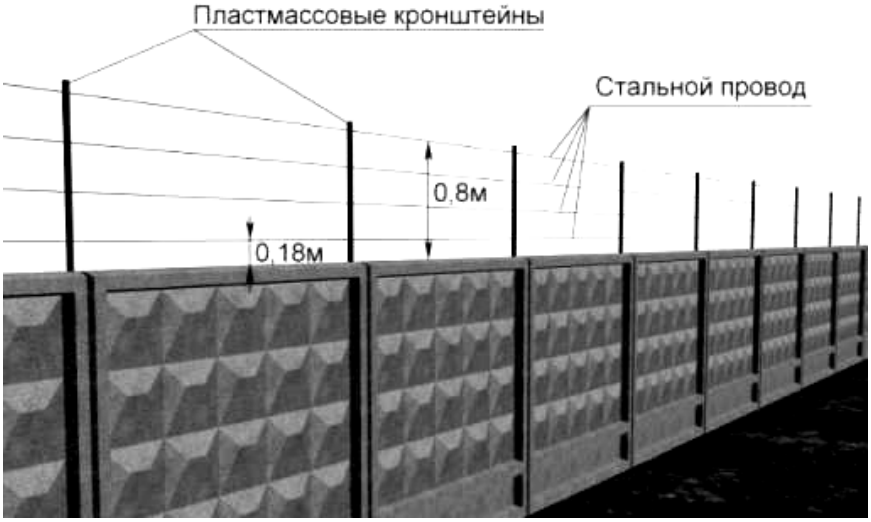


Рис. 5.25. Ёмкостное средство обнаружения «Радиан-14»

Принцип действия прибора основан на регистрации изменения электрической емкости сигнализационного заграждения относительно земли. Изменение этой емкости на величину, превышающую установленный уровень, вызывает срабатывание прибора. Отличительной особенностью прибора является наличие дополнительного (активного) канала, позволяющего компенсировать сигналы, возникающие при воздействии на СЗ внешних факторов в виде дождя или мокрого снега.

Обеспечивается функционирование в составе комплексов охранной сигнализации совместно с системами сбора и обработки информации, имеющими контактный вход, или автономно с простейшими звуковыми сигнализаторами. Предусмотрена возможность осуществления дистанционного контроля работоспособности прибора. Длина охраняемого рубежа – до 500 м.

Радиолучевые охранные системы

Радиолучевые охранные системы являются одними из основных средств предупреждения проникновения нарушителей вокруг больших охраняемых объектов. Их отличительной особенностью является всепогодность, обеспечение охранных функций в условиях дня и ночи, при любых метеоусловиях и во время катаклизмов.

Принцип действия радиолучевых охранных систем основан на формировании между передающим и приемным блоками, их антеннами электромагнитного поля, которое представляет собой чувствительную среду, регистрирующую появление объекта внутри данной зоны регистрации.

Такие радиолучевые охранные системы могут быть как объемными, так и протяженными, регистрирующими прохождения нарушителей через протяженное электромагнитное поле. В протяженных системах регистрирующее поле формируют как можно тоньше в виде электромагнитного забора Дальность действия таких электромагнитных заборов составляет от единиц до сотен метров.

Перекрытие площади поперечного сечения электромагнитного луча телом нарушителя можно представить формулой [20]:

$$P_{up} = \beta_0 (1+m) P_u ,$$

где P_u – мощность сигнала передатчика на выходе передающей антенны; P_{up} – мощность полезного сигнала на входе приемной антенны; β_0 – коэффициент передачи радиолокационного сигнала при отсутствии нарушителя; m – коэффициент модуляции полезного сигнала нарушителем.

При движении нарушителя в полный рост (m=0,5 – 0,9) изменение $\beta_0(1+m)$ составляет 3–10 дБ. При перемещении нарушителя ползком (m = 0,1 – 0,25) изменение $\beta_0(1+m)$ составляет 0,4–1,0 дБ.

Фиксация тревожного сигнала осуществляется на основе анализа изменений амплитуды и фазы принимаемого сигнала, возникающих при появлении в зоне постороннего предмета.

Рис. 5.26. Радиолучевая система ERMO 482

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

Широкий спектр радиолучевых охранных приборов выпускает итальянская компания CIAS. Приборы серии Ermusa отличаются компактностью и предназначены для использования как в помещениях, так и на улице для барьеров протяженностью 40–80 м. На рис. 5.26 показаны блоки радиолучевой системы ERMO 482 фирмы CIAS [57]. Приборы выпускаются в нескольких модификациях – для рубежей протяженностью 50, 80, 120 и 200 м. Используемые в блоках параболические антенны обеспечивают малую

расходимость луча, что позволяет использовать эту систему даже в условиях интенсивного городского движения. Частота излучения передатчика – 10,58 ГГц, питание – от аккумуляторной батареи или сетевого адаптера. Диаметр блока – 310 мм, глубина – 270 мм, масса – 3 кг. Блоки монтируются на сборных металлических штангах, позволяющих устанавливать излучатель и приемник на высоте до 1 метра. Со штангой конструктивно объединена коробка для блока питания и аккумулятора. Диапазон рабочих температур –25° до +55 °С.

Радиолучевые системы обеспечивают только одну зону охраны и применяются на прямолинейных участках периметра. На участках с непрямолинейной границей или при сложном рельефе местности нужно использовать многозонную систему, состоящую из нескольких комплектов аппаратуры.

Радиоволновые охранные системы

Принцип работы радиоволновой охранной системы основан на регистрации возмущений электромагнитного поля, которые создает попадающий в это поле нарушитель.

В простейшем случае система, например Рафид, содержит пару расположенных параллельно излучающих фидеров (ИФ), один из которых является передающей, а другой – приемной антенной радиочастотного поля (рис. 5.27). Выходной сигнал приемника непрерывно контролируется анализатором.

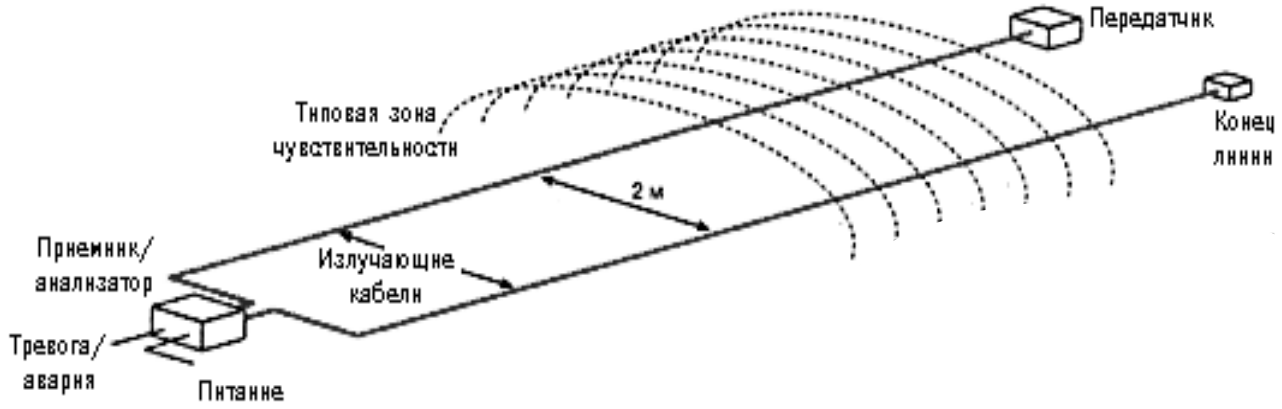


Рис. 5.27.Схема расположения излучающих фидеров

ИФ представляет собой специально сконструированный коаксиальный кабель, содержащий внутренний провод, изолированный диэлектриком от внешнего экрана. Внешний экран имеет так называемые «порты» или отверстия в экране, расположенные с регулярными интервалами. Такая конструкция кабеля обеспечивает излучение электромагнитного поля при пропускании по нему тока.

К одному из кабелей приложено высокочастотное напряжение постоянной амплитуды; этот кабель является простейшей антенной, излучающей

сигнал по всей длине. Второй кабель является приемной антенной, в нем наводится небольшой сигнал постоянной амплитуды от передающего кабеля.

Любой предмет, попавший в поле излучения, изменяет напряжение, наводимое во втором кабеле. Когда человек, тело которого содержит большое количество воды, движется в зоне поля, в приемном кабеле возникает сильный сигнал. Высокое отношение сигнала к шуму в этом случае позволяет обнаружить вторжение в охраняемую зону и обнаружить сигнал тревоги.

Кабели располагаются параллельно друг другу и монтируются на жесткой стене или другом ограждении, обеспечивая зону детектирования.

Электрошоковые системы охраны периметров

К устройствам активной охраны периметров относятся электрошоковые системы. Они предназначены для защиты периметров объектов от незаконного проникновения нарушителей. Принцип работы систем основан на легком воздействии электрических импульсов высокого напряжения на нарушителя при соприкосновении его с ограждением. При обрыве или замыкании нитей ограждения вырабатывается сигнал «Тревога».

В большинстве электрошоковых систем сочетаются одновременно физическое препятствие и сигнализационная система, что позволяет экономить средства при защите объекта.

Электрошоковое средство охраны периметра представляет собой ограждение с изолирующими опорами, на которых закреплены оголенные электропровода, соединенные с электронным блоком (контроллером). Контроллер вырабатывает электроимпульсы высокого напряжения, которые оказывают нелетальное воздействие на нарушителя. В результате воздействия на ограждение (замыкание или обрыв проводов) активизируется сигнал тревоги, который поступает на охранную панель.

Параметры системы (количество проводов, расстояние между ними, длина контролируемой зоны) являются различными и выбираются в соответствии с требованиями по охране объекта. Система позволяет создавать проводные электризуемые ограждения различной конфигурации:

- на заборы любого типа в виде козырька;
- по верху стен и крыш в виде козырька;
- совместно с существующим ограждением в виде второго забора;
- как отдельно стоящий забор.

Вопросы для самопроверки

1. Перечислите категории объектов, подлежащих охране.
2. Что относят к техническим средствам физической защиты информации?
3. Основные задачи, решаемые физическими средствами защиты.
4. Состав системы обеспечения безопасности объектов.
5. Что входит в состав системы охранно-тревожной сигнализации?
6. Что входит в состав системы контроля и управления доступом?
7. Что входит в состав системы пожарной сигнализации и пожаротушения?
8. Перечислите возможный состав периметровой охраны.
9. На каких принципах базируется обеспечение безопасности объекта?
10. Что предусматривают адекватные меры защиты?
11. Назначение системы охранно-тревожной сигнализации.
12. Назначение датчиков системы охранной сигнализации.
13. Средства, применяемые для записи видеосигналов.
14. Разделение охранных извещателей по физическому принципу действия.
15. Назовите основные типы извещателей.
16. Принципы действия пожарных извещателей.
17. Функции системы контроля и управления доступом на объекте.
18. Назначение системы пожарной сигнализации (ПС).
19. Какого типа бывают пожарные оповещатели?
20. Перечислите функциональные зоны охраны объекта.
21. В каких случаях применяются периметровые средства охраны?
22. Требования к периметровой системе охраны.
23. Принципиальные преимущества тепловизионных средств наблюдения за объектами.
24. Принцип действия емкостного средства обнаружения нарушителя.
25. Принцип действия радиолучевых охранных систем.
26. Принцип работы радиоволновой охранной системы.

6. ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Цели и задачи технического контроля эффективности мер защиты информации

Аттестация по требованиям безопасности информации предшествует разрешению на обработку подлежащей защите информации и официально подтверждает эффективность совокупности применяемых на конкретном объекте информатизации мер и средств защиты информации.

Комплекс специальных аттестационных мероприятий называется аттестационной проверкой и включает в себя *контроль эффективности защиты* – проверку соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации. *Показатель эффективности защиты информации* представляет собой меру или характеристику для ее оценки.

Нормы эффективности защиты информации соответствуют показателям, установленным нормативными документами.

Под *методом контроля эффективности защиты информации* понимают порядок и правила применения расчетных и измерительных операций при решении задач контроля эффективности защиты.

Виды контроля эффективности защиты делятся на:

– *организационный контроль* – проверка соответствия мероприятий по технической защите информации требованиям руководящих документов;

– *технический контроль* – контроль эффективности технической защиты информации, проводимый с использованием технических средств контроля. Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что утечка информации с объекта невозможна, т.е. на объекте отсутствуют технические каналы утечки информации. Технический контроль состояния защиты информации в системах управления производствами, транспортом, связью, энергетикой, передачи финансовой и другой информации осуществляется в соответствии со специально разрабатываемыми программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством по подчиненности объекта контроля.

По способу проведения и содержанию технический контроль эффективности технической защиты информации относится к наиболее сложным видам контроля и может быть:

- *комплексным*, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;

• *целевым*, когда проводится проверка по одному из интересующих каналов возможной утечки информации;

• *выборочным*, когда из всего перечня технических средств на объекте для проверки выбираются только те, которые по результатам предварительной оценки с наибольшей вероятностью имеют опасные каналы утечки защищаемой информации.

В зависимости от вида выполняемых операций методы технического контроля делятся на:

• *инструментальные*, когда контролируемые показатели определяются непосредственно по результатам измерения контрольно-измерительной аппаратурой;

• *инструментально-расчетные*, при которых контролируемые показатели определяются частично расчетным путем и частично измерением значений некоторых параметров физических полей аппаратными средствами;

• *расчетные*, при которых контролируемые показатели рассчитываются по методикам, содержащимся в руководящей справочной литературе.

С целью исключения утечки информации не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на средствах и информационных системах, находящихся в процессе обработки информации.

Технический контроль состояния защиты информации в автоматизированных системах управления различного назначения осуществляется в полном соответствии со специально разработанными программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством, которому подчиняется объект контроля.

Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что на объекте отсутствуют технические каналы утечки информации.

Контроль состояния защиты информации заключается в проверке соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием *технических и программных средств контроля.*

Средство контроля эффективности защиты информации – техническое, программное средство, вещество и/или материал, используемые для контроля эффективности защиты информации.

Технический контроль определяет действенность и надежность принятых мер защиты объектов информатизации от воздействия технических средств разведки.

Технический контроль предназначен для:

- выявления возможных каналов утечки конфиденциальной информации;
- проверки соответствия и эффективности принятых мер защиты нормативным требованиям;
- разработки рекомендаций по совершенствованию принятых защитных мероприятий.

Технический контроль проводится по отдельным физическим полям, создаваемых объектами информатизации, и состоит из:

- сбора исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки;
- определения возможных типов и средств технической разведки;
- предварительного расчета зон разведдоступности;
- определения состава и подготовки к работе контрольно-измерительной аппаратуры;
- измерения нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны;
- определения эффективности принятых мер защиты и в отдельных случаях разработки необходимых мер усиления защиты.

Для проведения технического контроля требуется наличие норм эффективности защиты, методик (методов) проведения контроля и соответствующей контрольно-измерительной аппаратуры.

Все контролируемые нормативные показатели разделяются на *информационные и технические* [5].

Информационные показатели относятся к вероятности обнаружения, распознавания и измерения технических характеристик объектов с заданной точностью.

Техническими показателями эффективности принятых мер защиты являются количественные показатели, характеризующие энергетические, временные, частотные и пространственные характеристики информационных физических полей объекта. Примерами таких характеристик могут быть напряженности электрического и магнитного полей ПЭМИ средств вычислительной техники, уровень сигналов наводок в силовых и слаботочных линиях за пределами контролируемой зоны, уровни акустических сигналов за пределами ограждающих конструкций и т.д. Нормой эффективности принятых мер защиты считается максимально допустимое значение контролируемых параметров на границе контролируемой зоны (в местах возможного нахождения технических средств разведки).

Инструментально-расчетные методы применяются тогда, когда комплект контрольно-измерительной аппаратуры не позволяет получить сразу конечный результат или не обладает достаточной чувствительностью.

Расчетные методы технического контроля применяются в случае отсутствия необходимой контрольно-измерительной аппаратуры, а также при необходимости быстрого получения предварительных ориентировочных результатов о зонах разведдоступности, например, перед инструментальными аттестациями рабочих мест.

При проведении технического контроля требуется контрольно-измерительная аппаратура, которая в большинстве случаев обеспечивает получение объективных характеристик контролируемых параметров или исходных данных для получения инструментально-расчетных характеристик. Контрольно-измерительная аппаратура по возможности должна быть портативной, что важно для аттестующих организаций, иметь достаточную чувствительность, соответствующую чувствительности аппаратуры разведки, быть надежной в эксплуатации.

Как правило, при проведении контроля расчетно-инструментальным методом проводится большое число измерений на дискретных интервалах и соответственно большое число сложных расчетов, что приводит к быстрой утомляемости испытателей. Поэтому современная тенденция развития контрольно-измерительной аппаратуры заключается в разработке для целей контроля программно-аппаратных комплексов, обеспечивающих полную автоматизацию измерения параметров физических полей и расчета нормируемых показателей защищенности объекта.

По результатам контроля состояния и эффективности защиты информации составляется заключение с приложением протоколов контроля.

6.2. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ

Типовой объект вычислительной техники (ВТ) – это средство вычислительной техники (СВТ) в типовой комплектации (например ПЭВМ в составе – системный блок, монитор, клавиатура, мышь, принтер), размещенное в отведенном для него помещении.

Для проведения специальных исследований типового объекта ВТ на ПЭМИ необходимы следующие документальные данные по объекту:

- предписание на эксплуатацию СВТ из состава объекта ВТ;
- план-схема КЗ объекта;
- схема расположения объекта ВТ внутри контролируемой зоны (КЗ);
- схема расположения основных технических средств и систем (ОТСС) и вспомогательных средств и систем (ВТСС) на объекте;

- схема размещения технических средств защиты информации (ТСЗИ) от утечки за счет ПЭМИ (если они установлены на объекте);
- сертификаты соответствия ТСЗИ;
- акт категорирования объекта ВТ.

Из анализа исходных данных должно быть установлено:

- заявленная категория объекта ВТ;
- состав ОТСС объекта (например ПЭВМ в типовой комплектации);
- ближайшие к объекту ВТ места возможного размещения стационарных, возимых, носимых средств разведки ПЭМИН;
- измеренные на объекте расстояния от ОТСС объекта ВТ до мест возможного размещения средств разведки ПЭМИН (Rкз, м);
- величины предельных расстояний (R2) от ОТСС объекта ВТ до мест возможного размещения средств разведки (из предписания на эксплуатацию СВТ);
- опасные режимы работы СВТ (обработки защищаемой информации);

Настоящая методика определяет виды контроля защищенности от разведки побочных электромагнитных излучений и наводок (РПЭМИН), порядок и способы его проведения на объектах информатизации [51].

Контроль защищенности осуществляется с целью предупреждения возможности получения аппаратурой РПЭМИН информации, циркулирующей на защищаемом от РПЭМИН объекте, и оценки эффективности мероприятий по противодействию РПЭМИН.

Контроль защищенности объекта предполагает проверку всех основных технических средств, средств защиты и вспомогательных технических средств, содержащих в своем составе генераторы, способные создавать электромагнитые излучения с модуляцией информационным сигналом. Основные и вспомогательные технические средства в дальнейшем для краткости будут именоваться как «технические средства».

Устройство считается защищенным, если на границе КЗ отношение «информативный сигнал/помеха» не превышает предельно допустимого значения δ как для побочных излучений, так и для наводок в цепях питания, заземления, линиях связи и т. д.. Объект считается защищенным, если защищено каждое устройство объекта.

Различается два вида контроля защищенности объектов от РПЭМИН:

– аттестационный контроль,

– эксплуатационный контроль.

Аттестационный контроль проводится при вводе объекта в эксплуатацию и после его реконструкции или модернизации, а эксплуатационный – в процессе эксплуатации объекта.

При проведении контроля защищенности проверяются параметры, которые характеризуют защищенность технических средств или объекта в целом в соответствии с установленной категорией объекта защиты.

Оценка защитных мероприятий электронных средств обработки информации состоит в проверке следующих возможных технических каналов утечки:

- побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами, на посторонние провода и линии, на цепи заземления и электропитания, выходящие за пределы контролируемой зоны;
- модуляции тока потребления технических средств информативными сигналами;
- радиоизлучений или электрических сигналов от возможно внедренных закладочных устройств в технические средства и выделенные помещения.

Технический контроль выполнения норм защиты информации от утечки за счет ПЭМИН по каждому перечисленному каналу утечки проводится для всех электронных устройств объекта ВТ.

Аттестационный контроль

Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, контрольную аппаратуру и тестовые средства, приводящие к минимальной погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

Аттестационный контроль состоит из организационной и инструментальной частей. В организационной части аттестационного контроля необходимо [51]:

- изучить план-схему местности, границы контролируемой зоны объекта и места возможного ведения разведки ПЭМИН с указанием средств (носимых, возимых, стационарных);
- уточнить категорию объекта информатизации, особенности его расположения, характер циркулирующей на объекте информации, в том числе и речевой, время её обработки техническими средствами;
- зафиксировать фактический состав основных и вспомогательных технических средств и средств защиты на объекте и поэкземплярно указать в перечне технических средств;
- уточнить план реального размещения технических средств на объекте и указать на нем кратчайшие расстояния от каждого технического средства и средства защиты до мест возможного ведения РПЭМИН;

• проверить визуально в доступных местах с возможным привлечением к этой работе штатных сотрудников организации выполнение монтажа коммуникаций, устройство заземления и электропитания на объекте защиты на соответствие проекту и СТР;

• проверить выполнение требований эксплуатационной документации по размещению и установке на объекте каждого технического средства и средства защиты с учетом расстояний до мест возможного ведения РПЭМИН;

• проверить обоснованность применения средств активной защиты (САЗ) и выполнение рекомендаций по их размещению;

• проверить наличие приемо-сдаточных документов и в доступных местах проверить правильность монтажа экранирующих средств на соответствие требованиям эксплуатационной документации и СТР.

Проверке подлежат следующие исходные данные и документация [51]:

• техническое задание на объект информатизации или приказ о начале работ по защите информации;

• технический паспорт на объект информатизации;

• приемо-сдаточная документация на объект информатизации;

• акты категорирования технических средств и систем;

• акт классификации АС по требованиям защиты информации;

• состав технических и программных средств, входящих в АС;

• планы размещения основных и вспомогательных технических средств и систем;

• состав и схемы размещения средств защиты информации;

• план контролируемой зоны учреждения;

• схемы прокладки линий передачи данных;

• схемы и характеристики систем электропитания и заземления объекта информатизации;

• описание технологического процесса обработки информации в АС;

• технологические инструкции пользователям АС и администратору безопасности информации;

• инструкции по эксплуатации средств защиты информации;

• предписания на эксплуатацию технических средств и систем;

• протоколы специальных исследований технических средств и систем;

• акты или заключения о специальной проверке выделенных помещений и технических средств;

• сертификаты соответствия требованиям безопасности информации на средства и системы обработки и передачи информации, используемые средства защиты информации;

• данные по уровню подготовки кадров, обеспечивающих защиту информации;

• данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;

• нормативная и методическая документация по защите информации и контролю ее эффективности.

В инструментальной части аттестационного контроля необходимо провести следующие работы:

• измерить или рассчитать для технических средств значения схемно-конструктивных параметров, характеризующих их защищенность от РПЭМИН (перечень этих параметров и методики их измерения указывается в эксплуатационной документации на эти технические средства);

• определить реальные размеры зоны R2 технических средств, установленных на объекте, по соответствующим методикам из сборника методик инструментального контроля в следующих случаях:

−для технических средств с неизвестными размерами зоны R2,

−для технических средств, эксплуатируемых на объектах, если размеры зоны R2 этих технических средств соизмеримы с расстоянием до мест возможного ведения РПЭМИ;

• проверить работоспособность всех средств защиты, включая САЗ, по методикам, приведенным в эксплуатационной документации на эти средства;

• определить эффективность применения САЗ для защиты АСУ и ЭВТ в соответствии с «Дополнением к Методике контроля защищенности объектов ЭВТ».

В случае положительных результатов предыдущих измерений формируются исходные данные для проведения эксплуатационного контроля защищенности от РПЭМИН технических средств АСУ и ЭВТ. С этой целью при отключенных средствах активной защиты измеряется уровень побочных электромагнитных излучений от технических средств АСУ и ЭВТ на двух-трех частотах с максимальным значением зоны R2 (реперные точки).

Частоты реперных точек, измеренные значения напряженности электрических и магнитных полей, типы и расположение антенн, а также другие условия проведения измерений фиксируются и используются при эксплуатационном контроле защищенности от РПЭМИН технических средств АСУ и ЭВТ.

По результатам аттестационного контроля для данного объекта оформляется Аттестат соответствия.

Технический контроль проводится путем запуска на ЭВМ специальной тестовой программы типа «Зебра», замера аппаратурой контроля излучаемых ЭВМ сигналов и последующим сравнением их с нормируемыми значениями.

Порядок инструментального контроля ПЭМИН:

• Измерение уровней ПЭМИ и наводок информативных сигналов:

– электрической составляющей;

– магнитной составляющей;

– индуктивной составляющей наводок в симметричных и несимметричных линиях как гальванически связанных, так и не связанных с проверяемым устройством, но имеющих выход за границы контролируемой зоны (если не выполняются требования предписания на эксплуатацию по зоне r1);

– измерение реального затухания в опасных направлениях на границе контролируемой зоны;

– измерение параметров применяемых средств защиты (фильтры в отходящих линиях, системы активного зашумления и т.д.).

• Расчет выполнения норм и оценка защищенности.

• Оформление протоколов по результатам проведенных проверок.

Контроль проводится для устройств, обрабатывающих или передающих информацию, представленную в последовательном коде. Измерения проводятся выборочно для частот, которые при специсследованиях дали максимальные значения зоны R2. Аналогично проводятся измерения эффективности систем активной защиты.

Если значения зоны R2 близки или превышают расстояние до границы контролируемой зоны (охраняемой территории), проводятся измерения реального затухания в опасном направлении, после чего производится расчет значений на границе контролируемой зоны. Измерения реального затухания проводится отдельно для каждого значения частоты сигнала.

Реальное затухание исследуемой линии в опасном направлении определяется по приведенной ниже схеме (рис. 6.1).

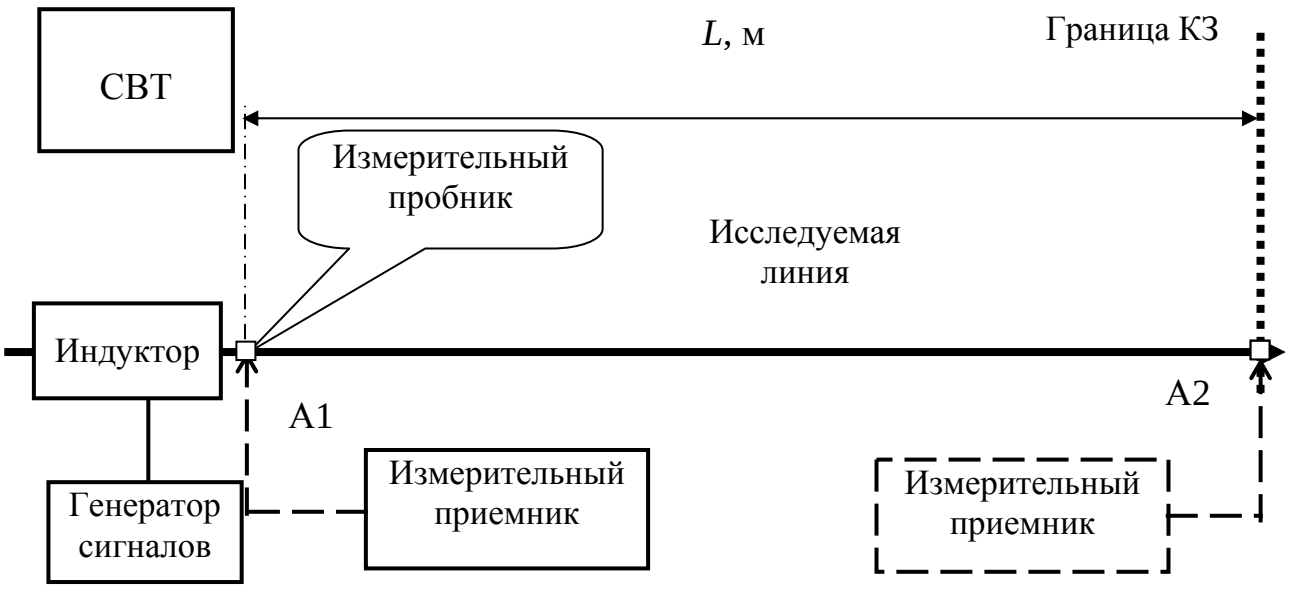


Рис. 6.1. Схема измерения реального затухания в линии

На каждой *j*-й частоте в исследуемую линию вблизи СВТ подают сигнал от вспомогательного источника и измеряют напряжение этого сигнала пробником напряжения в двух точках: вблизи СВТ в точке А1 (напряжение U_{1uj}) и на границе контролируемой зоны А2 (напряжение U_{2uj}). Коэффициент затухания вычисляют по формуле:

$$K_{лj} = \frac{U_{1uj}}{U_{2uj}}$$

При помощи измерительного приемника можно получить данные для расчета реального коэффициента затухания по ПЭМИ.

Для распределенных систем (например, локальных вычислительных сетей) проводятся исследования характеристик линий, по которым передается информации, по специальной методике расчета контролируемой зоны от экранированных кабелей связи АСУ и ЭВМ.

Применение неэкранированных кабелей для связи ЭВМ не допускается.

Эксплуатационный контроль

Эксплуатационный контроль защищенности от РПЭМИН на объекте предназначен для проверки выполнения правил эксплуатации и технического состояния каждого технического средства и оценки соответствия текущего состояния защищенности объекта и зафиксированного при аттестационном контроле.

Эксплуатационный контроль состоит из двух частей: организационной и инструментальной.

При выполнении организационной части эксплуатационного контроля необходимо [51]:

- проверить наличие Аттестата соответствия, журнала учета проведения эксплуатационного контроля, перечня и плана размещения технических средств на объекте;
- уточнить места возможного ведения РПЭМИ и при необходимости внести изменения в план-схему контролируемой зоны;
- проверить поэкземплярно соответствие реального состава технических средств и состава, указанного в перечне технических средств на объекте, а также регулярность проведения их эксплуатационного контроля по журналу учета проведения эксплуатационного контроля;
- сверить соответствие действительного расположения технических средств и средств защиты расположению, приведенному в плане размещения технических средств на объекте и в доступных местах выполнение требований по монтажу каждого технического средства и его коммуникаций, приведенных в эксплуатационной документации и СТР;
- проверить соответствие сведений о степени секретности обрабатываемой информации и установленной категории объекта совместно с представителем режимной службы предприятия.

В инструментальной части эксплуатационного контроля необходимо:

- для средств защиты и технических средств произвести измерения параметров защищенности от РПЭМИ, которые были определены на этапе аттестационного контроля;
- для технических средств АСУ и ЭВТ измерить напряженность электрических и магнитных полей в реперных точках и результаты измерений сравнить с результатами аттестационного контроля;
- проверить работоспособность средств активной защиты согласно указаниям в эксплуатационной документации на эти средства.

В случае положительных результатов эксплуатационный контроль объекта считается завершенным, о чем составляется Акт проведения эксплуатационного контроля на объекте. При выявлении недостатков последние устраняются и контроль повторяется.

При проведении эксплуатационного контроля на объекте допускается проведение работ выборочно относительно отдельных технических средств.

6.3. Методы испытаний

Общие положения [51]

1.1. Испытания ПЭВМ и периферийных устройств на соответствие нормам ПЭМИН проводят в соответствии с требованиями ГОСТ 51320-99.

1.2. ПЭВМ испытывают в составе базового комплекта (по ГОСТ 27201) и всех периферийных устройств, предусмотренных технической документацией на ПЭВМ.

Периферийное устройство испытывают совместно с базовым комплектом ПЭВМ, удовлетворяющим нормам ПЭМИН, установленным для ПЭВМ конкретного класса.

1.3. Если ПЭВМ или периферийное устройство, испытываемое совместно с базовым комплектом ПЭВМ, содержит идентичные технические средства или идентичные модули, то допускается проводить испытания при наличии хотя бы одного технического средства (модуля) каждого типа.

1.4. При испытаниях периферийных устройств (кроме сертификационных) допускается применение имитатора базового комплекта ПЭВМ при условии, что имитатор имеет электрические характеристики реального базового комплекта в части высокочастотных сигналов и импедансов и не влияет на параметры электромагнитной совместимости.

1.5. Значение напряжения (напряженности поля) посторонних радиопомех на каждой частоте измерений, полученное при выключенном испытуемом устройстве, должно быть не менее чем на 10 дБ ниже нормируемого значения на данной частоте.

Допускается проводить измерения при более высоком уровне посторонних радиопомех, если суммарное значение полей, создаваемых испытуемым устройством, и посторонних радиопомех не превышает нормы.

1.6. При испытаниях расположение и электрическое соединение технических средств, входящих в состав испытуемого устройства, должны соответствовать условиям, приведенным в технической документации на ПЭВМ. Если расположение технических средств и соединительных кабелей не указано, то выбирают такое, которое соответствует типовому применению и при котором создаваемые испытуемым устройством ПЭМИН имеют максимальное значение.

1.7. При испытаниях должны использоваться соединительные кабели, требования к которым указаны в технической документации на ПЭВМ или периферийное устройство. Если допустимы различные длины кабелей, то выбирают такие, при которых создаваемые испытуемым устройством ПЭМИН имеют максимальное значение. При испытаниях допускается применять экранированные или специальные кабели для подавления ПЭМИН в тех случаях, когда это указано в технической документации на ПЭВМ или периферийное устройство.

1.8. Излишне длинные кабели сворачивают в виде плоских петель размером 30–40 см приблизительно в середине кабеля.

1.9. Если изменения режима работы ПЭВМ (периферийного устройства) оказывают влияние на уровень ПЭМИН, то испытания проводят при режиме, соответствующем максимальному уровню ПЭМИН.

1.10. Расположение технических средств испытуемого устройства и соединительных кабелей, а также режимы работы ПЭВМ должны быть указаны в протоколе испытаний.

Аппаратура и оборудование [51]

2.1. Измеритель ПЭМИН с квазипиковым детектором и детектором средних значений по ГОСТ Р-51319-99.

2.2. V – образный эквивалент сети по ГОСТ Р-51319-99, тип 5 – в полосе частот от 0,15 до 100 МГц.

2.3. Измерительные антенны – по ГОСТ Р-51319-99 . При измерении напряженности поля ПЭМИН в полосе частот от 30 до 1000 МГц используют линейный симметричный вибратор, в полосе частот от 0,15 до 30 МГц – штыревую антенну. Допускается использование биконических антенн.

2.4. Металлический лист для измерения напряжения ПЭМИН по ГОСТ 51320-99.

2.5. Набор металлических листов общей площадью, обеспечивающей размещение испытуемого комплекта ПЭВМ и измерительной аппаратуры для измерения напряженности поля ПЭМИН по п. 4.3. Допускается использовать перфорированные металлические листы или сетку с размером перфорации или ячеек не более 0,02×0,02 м.

2.6. Столы и поворотные платформы для размещения испытуемого устройства и измерительных приборов должны быть изготовлены из изоляционного материала.

Измерения напряжения ПЭМИН [51]

3.1. Размеры помещения для проведения измерений должны быть такими, чтобы расстояние от испытуемого устройства (включая все технические средства и соединительные кабели, входящие в состав испытуемого устройства) до остальных металлических предметов и токонесущих поверхностей (кроме металлического листа) было не менее 0,8 м.

3.2. Измерения проводят в экранированном помещении. Эффективность его экранирования и фильтрации сети электропитания в помещении должна быть такой, чтобы обеспечивать выполнение требований п. 1.5. При выполнении требований п. 1.5 допускается проведение испытаний в неэкранированном помещении.

Расположение аппаратуры при измерении напряжений полей, создаваемых ПЭВМ показано на рис. 6.2.

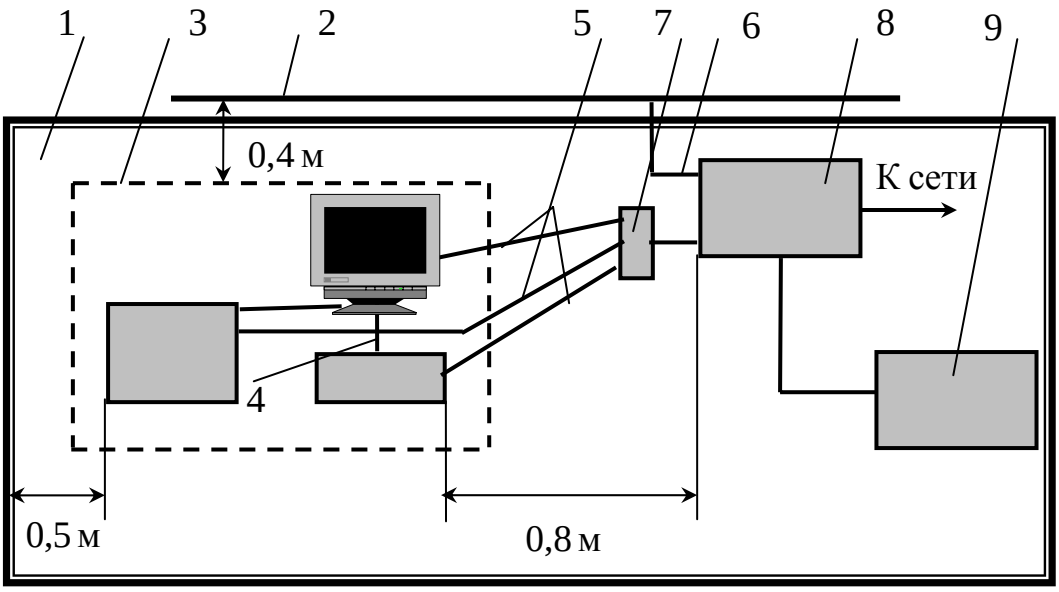


Рис. 6.2. Расположение аппаратуры при измерении напряжений полей, создаваемых ПЭВМ**:** *1* – стол; *2* – вертикально расположенный металлический лист; *3* – испытуемое устройство; *4* – межблочные соединения; *5* – сетевые кабели; *6* – шина заземления; *7* – штепсельная колодка; *8* – эквивалент сети; *9* – измеритель ПЭМИН

На столе, установленном у вертикально расположенной токопроводящей поверхности (металлического листа размером не менее 2×2 м или стены экранированного помещения), размещают ПЭВМ и эквивалент сети. Испытуемое устройство размещают на расстоянии 0,8 м от эквивалента сети и 0,4 м от металлического листа.

3.3. Эквивалент сети устанавливают непосредственно около токопроводящей поверхности и его корпус соединяют с этой поверхностью шиной

шириной не менее 0,005 м и минимально возможной длиной, но не более 0,4 м.

3.4. Если ПЭВМ имеет единственный сетевой кабель, то он подключается к эквиваленту сети.

Если ПЭВМ имеет более одного сетевого кабеля, то все они подключаются к штепсельной колодке, расположенной в непосредственной близости от эквивалента сети. Если длина сетевых кабелей превышает 1 м, то оставшиеся части кабелей сворачивают в соответствии с требованиями п. 1.8.

3.5. Расположение испытуемого устройства и измерительной аппаратуры при измерении напряжения ПЭМИН, создаваемых периферийным устройством, показано на рис. 6.3. Периферийное устройство размещают на расстоянии 0,8 м от эквивалента сети и 0,4 м от металлического листа. Сетевой кабель периферийного устройства подключают к эквиваленту сети. Сетевые кабели других технических средств, входящих в испытуемое устройство, подключают к сети электропитания.

3.6. Если по требованиям электробезопасности испытуемое устройство имеет специальные зажимы для подключения заземляющего провода, то заземляющий провод длиной 1 м прокладывают параллельно сетевому кабелю на расстоянии не более 0,1 м и подключают к зажиму заземления металлического листа.

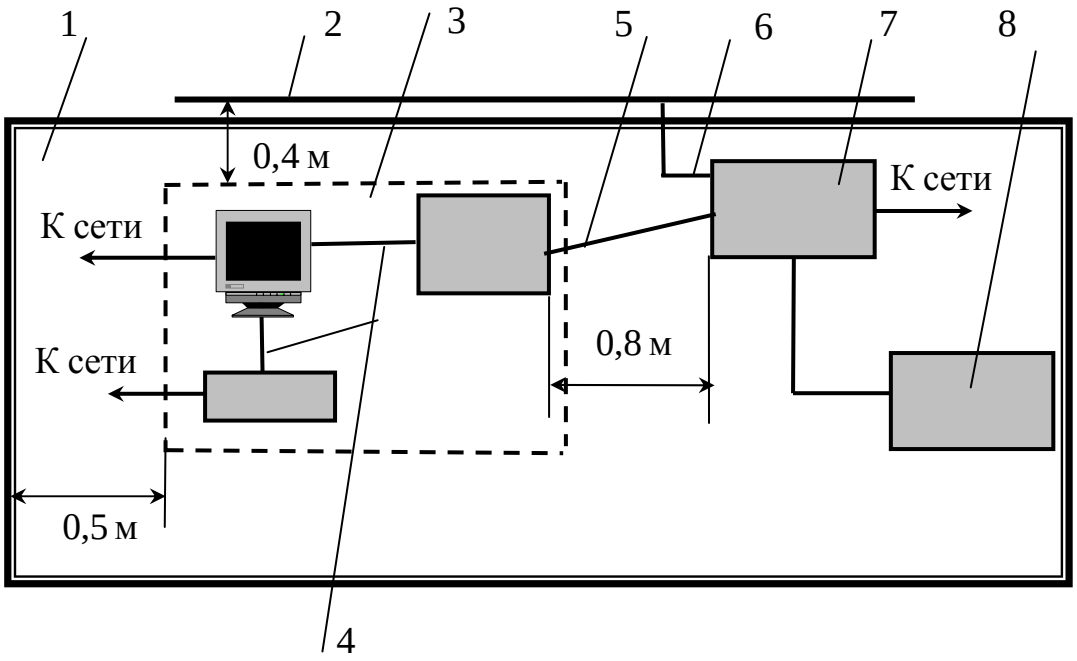


Рис. 6.3. Расположение аппаратуры при измерении напряжений полей, создаваемых периферийным устройством: *1* – стол; *2* – вертикально расположенный металлический лист; *3* – испытуемое устройство; *4* – межблочные соединения; *5* – сетевой кабель периферийного устройства; *6* – шина заземления; *7* – эквивалент сети; *8* – измеритель поля

3.7. При испытаниях проводят измерение квазипикового несимметричного напряжения ПЭМИН. За результат измерений на каждой частоте принимают наибольшее из значений, полученных для двух проводов.

3.8. Перед началом измерений, перестраивая измеритель ПЭМИН в пределах полосы нормирования, фиксируют частоты, на которых наблюдаются максимумы напряжения ПЭМИН. Измерения проводят на этих частотах. При большом числе таких частот допускается сократить их количество, но не менее чем до 10, выбрав те, на которых значения напряжения ПЭМИН наибольшие.

Измерения напряженности поля [51]

4.1. Измерения напряженности поля, создаваемых ПЭВМ или периферийным устройством, проводят на измерительной площадке, соответствующей требованиям ГОСТ 51320-99. Испытуемое устройство размещают на поворотной платформе на высоте 0,8 м над металлическим листом (рис. 6.4).

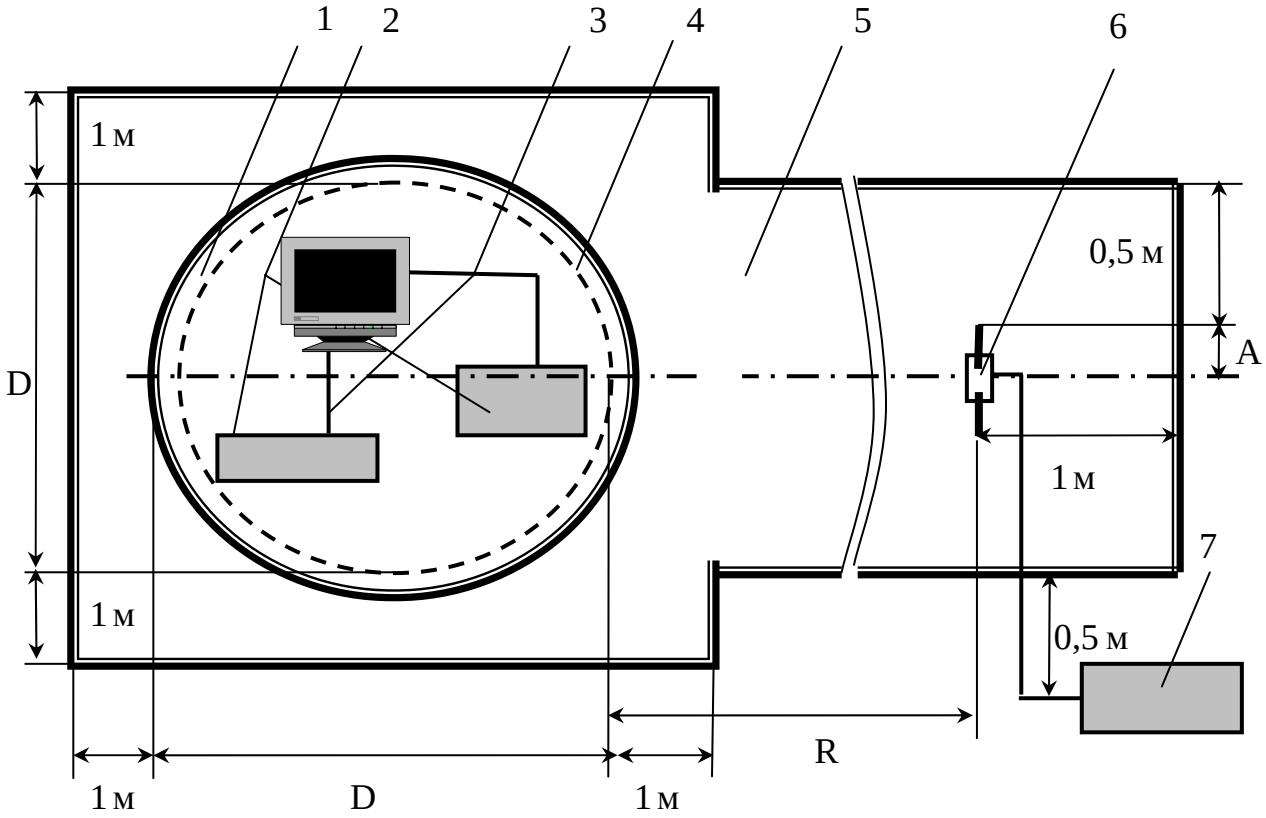


Рис. 6.4. Расположение аппаратуры при измерениях напряженности поля ПЭМИН, создаваемых испытуемым устройством: *1* – поворотная платформа; *2* – испытуемое устройство; *3* – межблочные соединения; *4* – граница испытуемого устройства; *5* – металлический лист; *6* – измерительная антенна; *7* – измеритель ПЭМИН; D – максимальный размер испытуемого устройства; *R* измерительное расстояние; A – максимальная длина антенны

4.2. Площадь под испытуемым устройством, между ним и измерительной антенной должна быть покрыта металлическими листами. Металличе-

ские листы должны выступать не менее чем на 1 м за границу испытуемого устройства с одного конца и не менее чем на 1 м за измерительную антенну с другого конца.

Границу испытуемого устройства представляет воображаемая линия, описывающая простую геометрическую фигуру, заключающую в себе технические средства испытуемого устройства. Все соединительные кабели должны быть включены в пределы этой геометрической фигуры.

4.3. При измерении напряженности поля ПЭМИН в полосе частот от 30 до 100 МГц используют эквивалент сети.

Сетевой кабель испытуемого устройства прокладывают кратчайшим путем вертикально вниз вдоль оси вращения поворотной платформы.

4.4. Расстояние *R* от проекции центра измерительной антенны на землю до границы испытуемого устройства должно соответствовать требованиям, указанным в Методике измерения побочных информативных сигналов, излучаемых техническими средствами АСУ и ЭВМ, но не менее 1 м.

4.5. При измерении напряженности поля ПЭМИН нижнюю точку штыревой антенны устанавливают на высоте 1 м, центр симметрии линейного симметричного вибратора – на высоте h, определяемой путем перемещения приемной антенны по вертикали вблизи исследуемого оборудования до положения, соответствующего максимуму принимаемого сигнала.

В полосе частот от 0,15 до 30 МГц определяют наибольшее квазипиковое значение вертикальной составляющей электрического поля ПЭМИН на частоте измерений при повороте платформы с испытуемым устройством.

В полосе частот от 30 до 1000 МГц определяют наибольшие квазипиковые значения горизонтальной и вертикальной составляющих электрического поля ПЭМИН на частоте измерений при повороте платформы с испытуемым устройством. За результат измерений на каждой частоте принимают наибольшее из полученных значений.

6.4. Порядок проведения контроля защищенности АС от НСД

В информационных системах и в автоматизированных системах обработки информации проверяются [51]:

- наличие сведений, составляющих государственную или служебную тайну, циркулирующих в средствах обработки информации и помещениях в соответствии с принятой на объекте технологией обработки информации;
- правильность классификации автоматизированных систем в зависимости от степени секретности обрабатываемой информации;
- наличие сертификатов на средства защиты информации;
- организация и фактическое состояние доступа обслуживающего и эксплуатирующего персонала к защищаемым информационным ресурсам,

наличие и качество организационно-распорядительных документов по допуску персонала к защищаемым ресурсам, организация учета, хранения и обращения с конфиденциальными носителями информации;

- состояние учета всех технических и программных средств отечественного и иностранного производства, участвующих в обработке защищаемой информации, наличие и правильность оформления документов по специальным исследованиям и проверкам технических средств информатизации, в том числе на наличие недекларированных возможностей программного обеспечения;
- обоснованность и полнота выполнения организационных и технических мер по защите информации;
- наличие, правильность установки и порядка эксплуатации средств защиты от несанкционированного доступа к информации;
- выполнение требований по технической защите информации при подключении автоматизированных систем к внешним информационным системам общего пользования.

В ходе проверки анализируется система информационного обеспечения объекта:

- используемые типы ЭВМ и операционных систем;
- виды и объемы баз данных;
- распределение закрытой и открытой информации по рабочим местам пользователей;
- порядок доступа к информации, количество уровней разграничения доступа;
- порядок поддержания целостности информации и резервного копирования.

Осуществляется проверка эффективности реально установленных механизмов защиты информации требованиям соответствующего класса защиты информации от НСД.

Структура систем защиты средств и систем информатизации от несанкционированного доступа должна включать в себя четыре подсистемы:

1. Подсистему управления доступом, которая осуществляет персонализацию действий в системе на основе идентификаторов и профилей пользователей (паспортов) отдельно для каждого уровня, а также разграничение доступа на их основе.

2. Подсистему учета и контроля, накапливающую и в дальнейшем обрабатывающую в журнале учета статистические сведения о доступе пользователей к различным ресурсам сети и возможных попытках НСД.

3. Криптографическую подсистему (для информации с грифом «СС» и выше) для шифрования конфиденциальной информации, записываемой на магнитные носители и передаваемой по линиям связи. Вся информация, не

подлежащая открытому распространению, шифруется непосредственно в ее источнике (рабочей станции, терминале, базе данных) и передается по открытым линиям связи в зашифрованном виде.

4. Подсистему обеспечения целостности, которая осуществляет контроль целостности средств операционных систем, прикладных программ и баз данных, а также средств защиты информации.

6.5. Методы контроля побочных электромагнитных излучений генераторов технических средств

Модуляция информационным речевым сигналом высокочастотных колебаний у генераторов технических средств может возникать из-за изменения индуктивностей и емкостей их задающих контуров под воздействием акустического поля. Перехват модулированных сигналов по каналу ПЭМИ с последующей демодуляцией приводит к утечке речевой информации.

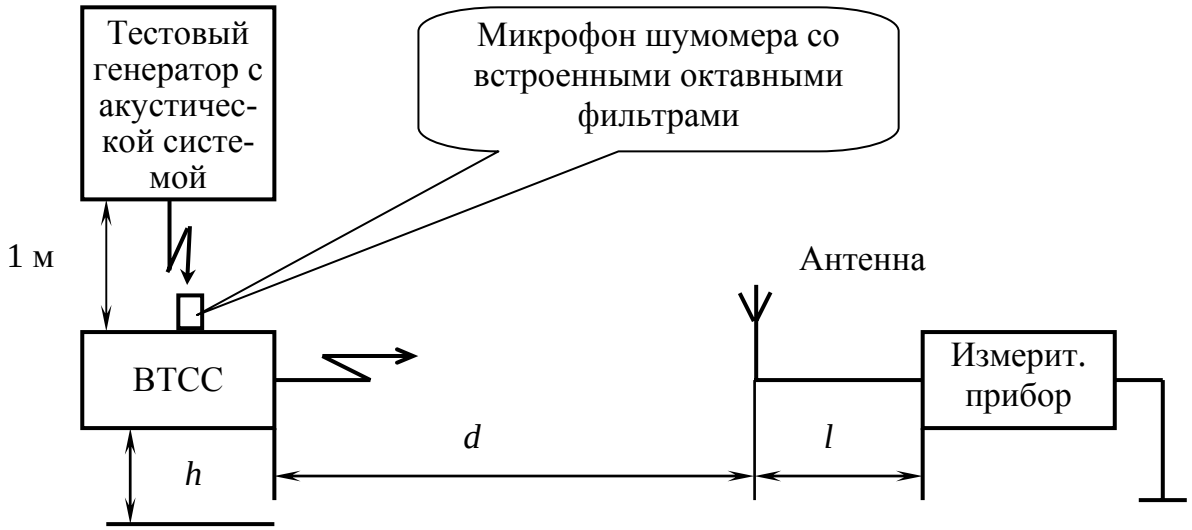


Рис. 6.5. Измерение побочных электромагнитных излучений ВТСС

Для исследования влияния акустического поля на техническое средство необходимо собрать установку по схеме рис. [52] и выполнить следующие действия.

- Установить измерительную антенну измерительного прибора на расстоянии d = 1м от исследуемого ВТСС на наиболее опасном с точки зрения перехвата сигнала направлении.
- Включить исследуемое ВТСС в штатный режим работы.
- Перестройкой измерительного приемника в исследуемом диапазоне частот, обнаружить сигналы, создаваемые генератором ВТСС.
- Настроить измерительный приемник на частоту наиболее мощного обнаруженного сигнала, которая, как правило, совпадает с частотой генератора. Полоса пропускания измерительного приемника устанавливается максимально близкой к ширине спектра сигнала генератора ВТСС.

• Акустическую систему излучателя генератора тестовых акустических сигналов разместить на расстоянии 1 м от исследуемого технического средства и направить в его сторону.

• В месте размещения ВТСС на расстоянии 1 м от излучателя акустической системы установить измерительный микрофон шумомера со встроенными октавными фильтрами.

• Включить акустическую систему и настроить ее на частоту f_1 = 1000 Гц. Установить необходимый уровень звукового давления: 80 дБ при наличии средств звукоусиления, 72 дБ – при их отсутствии.

При выявления факта наличия боковых составляющих спектра исследуемого сигнала делается вывод о наличии акустоэлектрических преобразований ВТСС. Измерить уровень их ПЭМИ.

Если боковые составляющие спектра исследуемого сигнала отсутствуют, то делается вывод об отсутствии акустоэлектрических преобразований в генераторе исследуемого ВТСС.

Если акустоэлектрические преобразования обнаружены, то необходимо:

• Провести измерение уровней напряженности электрического ($E_{\text{и}}$) и магнитного ($\rho H_{\text{и}}$) полей, создаваемых генератором, и ширину спектра сигнала ($\Delta F_{\text{с}}$) на частоте генератора.

• На частоте генератора ВТСС произвести измерения уровней напряженностей помех $E_{\text{п}j}$ и $\rho H_{\text{п}j}$. Измерения проводятся без изменения режима работы приемника.

• Произвести расчет значений уровня информативного сигнала $E_{\text{с}}$ и $\rho H_{\text{с}}$ по формулам [52]:

$$E_{\text{с}} = \sqrt{(\xi_{\text{и}} E_{\text{и}})^2 - (E_{\text{п}} / \xi_{\text{и}})^2}, \text{ мкВ/м}, \qquad (6.1)$$

$$\rho H_{\text{с}} = \sqrt{(\xi_{\text{и}} \rho H_{\text{и}})^2 - (\rho H_{\text{п}} / \xi_{\text{и}})^2}, \text{ мкВ/м}, \qquad (6.2)$$

где $E_{\text{с}}, \rho H_{\text{с}}$ – уровни информативного сигнала, мкВ/м; $\xi_{\text{а}}$ – погрешность входного преобразователя (погрешность коэффициента калибровки антенны), дБ; $\xi_{\text{и}} = 1 + \sqrt{(10^{0,05\xi_{\text{а}}} - 1)^2 + (10^{0,05\xi_{\text{ип}}} - 1)^2}$ – относительная среднеквадратичная ошибка измерения (в разах); $\xi_{\text{ип}}$ – погрешность измерительного приемника, дБ; $\rho = 377$ Ом – волновое сопротивление неограниченной среды (для вакуума $\rho = 120\pi = 377$ Ом).

• Через волновое сопротивление измерения напряженности магнитного поля из мкА/м пересчитываются в соответствующую напряженность электрического поля, измеряемую в мкВ/м.

• Измерить расстояние r в метрах от ВТСС до ближайшего места возможного расположения средств технической разведки за пределами кон-

тролируемой зоны. Рассчитать значение коэффициента затухания V_r по следующим формулам.

Если частота обнаруженного сигнала генератора ниже частоты $f \le 47{,}75\,\text{МГц}$, то коэффициент затухания рассчитывается по формуле:

$$V_r = \begin{cases} r^3, \text{ если } r \le \dfrac{47{,}75}{f}; \\ \dfrac{47{,}75}{f}, \text{ если } r \le \dfrac{47{,}75}{f} < r \le \dfrac{1800}{f}; \\ \dfrac{8{,}59 \cdot 10^4 r}{f^2}, \text{если } r > \dfrac{1800}{f}, \end{cases} \tag{6.3}$$

где f – частота измеренного сигнала, МГц.

Если частота обнаруженного сигнала генератора удовлетворяет условию $47{,}75\,\text{МГц} < f \le 1800\,\text{МГц}$, то коэффициент затухания определяется по формуле

$$V_r = \begin{cases} r^2, \text{ если } r \le \dfrac{1800}{f}; \\ \dfrac{1800r}{f}, \text{если } r > \dfrac{1800}{f}. \end{cases} \tag{6.4}$$

Если частота обнаруженного сигнала генератора удовлетворяет условию $f > 1800\,\text{МГц}$, то коэффициент затухания определяется по формуле:

$$V_r = r. \tag{6.5}$$

Рассчитать действующую высоту антенны h_a по формуле:

$$h_{\text{а}} = \frac{2}{10^{\frac{K_{\text{а}}^*}{20}}} \approx \frac{63 \cdot 10^{\frac{G_{\text{а}}^*}{20}}}{f}, \text{ м}, \tag{6.6}$$

где $K_{\text{а}}^*$ – антенный коэффициент (логарифмический), дБ относительно 1/м; f – частота сигнала, МГц; $G_{\text{а}}^* = 10\lg G_{\text{а}}$, дБ – коэффициент усиления антенны в относительных единицах, определяемый через коэффициент усиления антенны $G_{\text{а}}$, эффективную площадь антенны $S_{\text{а}}$ и длину волны сигнала λ как $G_{\text{а}} = 4\pi S_{\text{а}} / \lambda^2$.

• Рассчитать уровень шумов на входе радиоприемного устройства по формуле:

$$U_{\text{ш}} = \sqrt{\left(\frac{U_{\text{ш}}^{*2}}{\Delta F_{\text{п}}^{*} \cdot 10^{\frac{q^{*}}{10}}} + \frac{10^{\frac{E_{\text{а}}^{*} - K_{\text{а}}^{*}}{10}}}{\Delta F_{\text{а}}} \right) \Delta F_{\text{с}}} \qquad (6.7)$$

где $U_{\text{ш}}^{*}$ – чувствительность радиоприемного устройства, мкВ; $\Delta F_{\text{п}}^{*}$ – полоса пропускания тракта приемного устройства, при котором измерялась чувствительность, Гц; q^{*}– отношение сигнал/шум, при котором измерялась чувствительность приемного устройства, дБ; $E_{\text{а}}^{*}$ – чувствительность антенны, измеренная при $q^{*} = 1$ и полосе пропускания приемника ΔF, дБ относительно мкВ/м; K_a^{*} – антенный коэффициент (логарифмический), дБ относительно 1/м; $\Delta F_{\text{с}}$ – ширина спектра сигнала генератора, Гц; $\Delta F_{\text{а}}$ – полоса пропускания, при которой производилось измерение чувствительности антенны.

Рассчитать отношение сигнал/шум на входе разведывательного приемника по формулам:

для электрического поля

$$q_E = (E_{\text{с}} h_{\text{д}}) / (2 V_r U_{\text{ш}}); \qquad (6.8)$$

для магнитного поля

$$q_H = (\rho H_{\text{с}} h_{\text{д}}) / (2 V_r U_{\text{ш}}), \qquad (6.9)$$

где $E_{\text{с}}, \rho H_{\text{с}}$ – уровни информативного сигнала, мкВ/м; $U_{\text{ш}}$ – напряжение шумов на входе разведывательного приемника, мкВ; $h_{\text{д}}$ – действующая длина антенны разведывательного приемника, м.

Рассчитать предельно допустимое значение сигнал/шум по формуле:

$$\delta = (3{,}2 + \Phi^{-1}(x) P_{\text{п}}) / (3{,}16 - \Phi^{-1}(x) P_{\text{п}}), \qquad (6.10)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\frac{t^2}{2}) dt$ – интеграл вероятности; $\Phi^{-1}(x)$ – функция обратная $\Phi(x)$; $P_{\text{п}}$ – предельно допустимое значение вероятности правильного обнаружения сигнала средствами разведки.

Сравнить рассчитанные значения сигнал/шум q_E и q_H с предельно допустимым δ. При выполнении условия $q \le \delta$ считается, что перехват ПЭМИ ВТСС на частотах работы высокочастотного генератора средствами разведки невозможен.

В случае, если это неравенство не выполняется, то необходимо определить реальный коэффициент затухания сигнала V_r^{*} при его распространении от места проведения измерения до места возможного нахождения средств технической разведки на расстоянии r. Для этого необходимо [52]:

• вблизи ВТСС установить вспомогательный излучатель, состоящий из генератора синусоидального сигнала и излучающей электрической антенны, которую необходимо поместить вместо ВТСС;

• настроить генератор на частоту генерации ВТСС;

• установить измерительную антенну приемника на расстоянии d = 1 м от излучающей антенны вспомогательного излучателя, приемник настроить на частоту генератора, причем, полосы пропускания генератора и приемника должны быть приблизительно равны;

измерить уровень напряженности электрического поля от вспомогательного излучателя;

• установить измерительную антенну в месте предполагаемого размещения средств разведки и измерить расстояние r;

• измерить уровень напряженности электрического поля $E_{\text{г}}^{r}$ в этой точке от вспомогательного излучателя;

• при выключенном генераторе измерить уровень помех $E_{\text{п}}^{r}$;

• определить реальное затухание как $V_r^* = E_{\text{г}} \big/ E_{\text{г}}^{r}$;

• провести расчет отношения сигнал/шум на входе измерительного приемника по формуле $q_E^* = (q_E V_r) \big/ V_r$.

Далее по рассмотренной ранее методике определяются условия возможности или невозможности перехвата ПЭМИ ВТСС на частотах работы высокочастотного генератора.

6.6. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации

6.6.1. Общие положения

Технический контроль акустической защищенности выделенного помещения проводится в целях документального подтверждения реальной возможности утечки (или ее отсутствия) акустической информации из проверяемого помещения в рабочем режиме.

Технический контроль проводится относительно мест возможного размещения аппаратуры разведки:

• носимой – на границе контролируемой зоны;

• возимой – в местах возможного нахождения аппаратуры разведки (стоянки автомобилей, соседние здания или сооружения).

Контроль защищенности от случайного (непреднамеренного) прослушивания проводится относительно мест возможного пребывания лиц, не допущенных к конфиденциальной информации.

При оценке мероприятий по информационной защите помещений учитываются следующие возможные технические каналы утечки или нарушения целостности информации[51]:

- акустическое излучение речевого сигнала по воздушной среде;
- электрические сигналы, возникающие в результате преобразования акустических сигналов в электрические устройствами, обладающими микрофонным эффектом, и распространяющиеся по проводным линиям, выходящим за пределы контролируемой зоны;
- вибрационные сигналы, возникающие посредством преобразования акустических сигналов в колебания упругих сред ограждающих конструкций выделенных помещений;
- электромагнитные излучения случайных источников (паразитных генераторов), модулированные звуковым сигналом.

Для указанных технических каналов утечки информации существуют различные виды сред распространения сигналов таких как:

- проводные сети: электрические силовые, низковольтные (телефонные, охранные, пожарные, радиотрансляция, часофикация), сети ЭВМ (витая пара, коаксиал, волоконно-оптические), кабели спецсвязи;
- инженерные коммуникации: отопление, водопровод, канализация, короба и трубы кабельных коммуникаций, специальные проемы и отверстия в стенах и перекрытиях, воздуховоды приточные и вытяжные;
- элементы конструкции зданий: стены капитальные, перегородки, окна (рамы, стекла), двери и перегородки, потолки;
- воздушная среда, по которой распространяются электромагнитные излучения технических средств (модуляция случайных генераторов, акустоэлектрические преобразования, побочные электромагнитные излучения, переизлучения под воздействием внешних источников).

При проведении контроля проверяются следующие исходные данные и документация:

- техническое задание на объект информатизации;
- технический паспорт на объект информатизации;
- приемо-сдаточная документация на объект информатизации;
- акты категорирования выделенных помещений и технических средств и систем;
- состав технических средств, расположенных в выделенном помещении;
- планы размещения основных и вспомогательных технических средств и систем;
- состав и схемы размещения средств защиты информации;
- план контролируемой зоны предприятия (учреждения);
- схемы прокладки линий передачи данных;

• схемы и характеристики систем электропитания и заземления объекта информатизации;

• инструкции по эксплуатации средств защиты информации;

• предписания на эксплуатацию технических средств и систем;

• протоколы специальных исследований технических средств и систем;

• акты или заключения о специальной проверке выделенных помещений и технических средств;

• сертификаты соответствия требованиям безопасности информации на средства и системы обработки и передачи информации, используемые средства защиты информации;

• данные по уровню подготовки кадров, обеспечивающих защиту информации;

• данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;

• нормативная и методическая документация по защите информации и контролю ее эффективности.

Технический контроль проводится путем генерации в помещении специального тестового звукового сигнала заданного уровня, измерения его уровня за ограждающей конструкцией помещения в воздушной среде, строительных конструкциях и токопроводящих коммуникациях. По результатам измерений проводится расчет нормируемого показателя (словесной разборчивости речи) и сравнивается расчетное значение с допустимым значением.

Инструментальный контроль акустической защищенности выделенных помещений предполагает:

• измерение уровней:

– акустического сигнала за пределами помещения;

– виброакустического сигнала в строительных конструкциях и инженерных коммуникациях;

– электрических сигналов в токопроводящих коммуникациях, имеющих выход за пределы контролируемой зоны;

– проверка наличия паразитной генерации;

– измерение параметров применяемых средств защиты (системы активного акустического зашумления и т. д.);

• расчет выполнения норм и оценка защищенности;

• оформление протоколов по результатам проведенных проверок.

6.6.2. Подготовительный этап контроля

Подготовительному этапу соответствует качественная оценка вибро- и звукоизоляции помещения с целью выявления наиболее уязвимых мест с

точки зрения утечки речевой информации. Оценка должна содержать анализ архитектурно-планировочных и конструктивных особенностей помещения, устройства его ограждающих конструкций (стен, перекрытий, дверей, окон) и инженерно-технических систем (систем водо- и теплоснабжения, вентиляции), неоднородностей в ограждающих конструкциях. Обследованию подлежат также конструктивные особенности элементов отделки.

Далее определяется или уточняется степень конфиденциальности речевой информации и соответствие ее категории объекта защиты, а также соответствующее значение нормированного показателя противодействия речевой разведке, руководствуясь которым необходимо проводить инструментальный контроль.

Для уточнения условий речевой деятельности в контролируемом помещении проводится слуховой контроль звукоизоляции ограждающих конструкций путем прослушивания без инструментальных средств акустических сигналов из контролируемого помещения. В качестве таких сигналов рекомендуется использовать естественную речь нормальной громкости, записанную на магнитофон.

Оцениваются пространственные соотношения ограждающих конструкций помещения и элементов технических систем относительно границы контролируемой зоны и прилегающих к контролируемой зоне строительных объектов. Эти соотношения необходимы для использования в расчетах эффективности защиты.

Определяются места возможного съема информации лазерными средствами и направленными микрофонами, а также точки контроля для определения характеристик этих каналов утечки информации.

Для направленных микрофонов место съема информации находится непосредственно за ограждающей конструкцией помещения, видимое из-за границы контролируемой зоны. Расстояние возможного съема информации определяется чувствительностью аппаратуры технической разведки и устанавливается согласно данных ее модели.

Для средств лазерного съема информации контроль может производиться как прямым способом так и косвенным. Для применения прямого способа контроля необходимо иметь специальный имитатор ИК-излучения. Косвенный способ предполагает получение оценки по результатам измерения виброзащищенности оконных стекол выделенного помещения, выходящих на разведопасные направления. Оценка проводится как для наружных, так и для внутренних стекол. Для внутренних стекол оценка не обязательна, если между наружными и внутренними стеклами находится светозащитный материал, либо наружное стекло покрыто специальной светоотражающей пленкой.

Расстояние возможного съема информации определяется по данным модели инженерно-технической разведки для направлений, близких к нормальным (±30°) по отношению к поверхности стекла. Если к окнам возможен непосредственный доступ с неохраняемой территории, то для них разведопасными являются все направления.

Когда помещение расположено в здании высоко и для проведения контроля доступ снаружи к нему затруднен, то инструментальный контроль проводится на аналогичном окне, расположенном ниже, но имеющем аналогичные условия расположения по зашумленности (выходящем на ту же сторону здания).

Оценка защищенности акустической информации от случайного прослушивания, например, в приемной учреждения, проводится только по акустическому каналу.

6.6.3. Акустический и виброакустический контроль

Методика контроля

Методика инструментального контроля выполнения норм противодействия акустической речевой разведке основывается на инструментально-расчетном методе определения отношений «*речевой сигнал / акустический (вибрационный) шум» (*далее – *«сигнал/шум»*) в контрольных точках в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц. Полученные отношения «сигнал/шум» сравниваются с нормированными, или пересчитываются в числовую величину показателя противодействия для сравнения с нормированным значением. Методика ориентирована на использование контрольно-измерительной аппаратуры общего применения.

В случае применения специальных автоматизированных комплексов контроля выполнения норм противодействия акустической речевой разведке (Шорох, Спрут) технология проведения и обработки результатов всех измерительных операций должна приводиться в их эксплутационной документации. Автоматизированные комплексы контроля должны быть сертифицированы в установленном порядке. Контролируемым параметром для них является словесная разборчивость речи.

В качестве тестового (контрольного) сигнала необходимо использовать акустический шумовой сигнал с нормальным распределением плотности вероятности мгновенных значений в пределах каждой октавной полосы частот. Современные генераторы шума способны излучать контрольный сигнал одновременно во всех октавных полосах (в полосе частот 175…5600 Гц), либо последовательно в каждой отдельно взятой полосе. Для сокращения времени проведения контроля рекомендуется генерировать тестовый сигнал одновременно во всех октавных полосах.

При инструментальном контроле выполнения норм противодействия акустической речевой разведке допускается также использование гармонических (тональных) сигналов со среднегеометрическими частотами октавных полос. В этом случае в контрольной точке проводится не менее трех измерений на частотах $f_{ср} \pm \Delta f$, где $f_{ср}$ – среднегеометрическая частота октавной полосы частот; Δf – частотная поправка, равная (10…15)% от $f_{ср}$. Итоговый результат акустических (вибрационных) измерений в контрольных точках необходимо находить путем усреднения результатов отдельных измерений.

Определение числовых значений отношений «сигнал/шум» в контрольных точках необходимо проводить в периоды минимальной зашумленности мест речевой деятельности (отсутствие персонала в помещении, выключение шумящего технического оборудовании и т.п.). Лучше всего проводить контроль в ночное время.

Продолжительность измерения уровней звукового давления в каждой точке выбирается в зависимости от интенсивности транспортного потока, но так, чтобы за время не менее 60 с по улице или дороге прошло не менее 20 транспортных единиц.

Для проведения инструментального контроля при отсутствии автоматизированных комплексов должны быть созданы передающая и приемная измерительные системы на основе аппаратуры общего применения. Передающая измерительная система размещается в контролируемом помещении, а приемная – в контрольной точке.

Передающая измерительная система должна содержать:

– генератор шума;

– усилитель мощности;

– акустический излучатель;

– измерительный микрофон;

– измеритель шума (шумомер);

– полосовые октавные фильтры со среднегеометрическими частотами, 250, 500, 1000, 2000, 4000 Гц.

Приемная измерительная система должна включать в себя:

– измерительный микрофон;

– вибродатчик (акселерометр);

– измеритель шума и вибраций (шумомер);

– полосовые октавные фильтры со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.

Вместо шумомера в измерительных комплексах могут быть использованы спектральные анализаторы, а измерительный микрофон может поочередно использоваться в обеих системах.

Выбор контрольных точек и размещение элементов измерительных комплексов

Контрольными точками являются места возможной установки акустических и вибрационных датчиков аппаратуры акустической речевой разведки, места расположения отражающих поверхностей лазерного излучения, места непреднамеренного прослушивания речи, в которых производятся акустические измерения.

При контроле выполнения норм противодействия акустической речевой разведке с применением микрофонов (в том числе с применением направленных микрофонов) контрольные точки должны выбираться на расстоянии 0,5 м от внешних поверхностей обследуемой ограждающей конструкции.

В случае неоднородности ограждающей конструкции акустические измерения выполняются отдельно для каждого участка, а результат принимается по наихудшему случаю.

При проведении контроля выполнения норм противодействия речевой разведке с применением виброакустических средств необходимо учитывать также элементы инженерно-технических систем, попадающих в акустическое поле источников речевых сигналов.

Если граница контролируемой зоны проходит по ограждающим конструкциям выделенного помещения, то контрольные точки для вибрационных измерений выбираются *непосредственно* на внешних по отношению к источнику речевого сигнала поверхностях ограждающих конструкций. В случае неоднородной ограждающей конструкции вибрационные измерения необходимо выполнять отдельно для каждого участка и делать оценку по наихудшему случаю.

Если через границу контролируемой зоны проходят коммуникации инженерно-технических систем (чаще всего трубы тепло– и водоснабжения), то контрольные точки для вибрационных измерений выбираются *непосредственно* на поверхности этих элементов на расстоянии, не превышающем 0,5 м от места их входа и выхода.

Вибродатчики (акселерометры) должны иметь плотный контакт с поверхностями ограждающих конструкций и с различными конструктивными элементами инженерно-технических систем – при контроле защищенности от речевой разведки с использованием вибрационных средств и с плоскостями стекол оконных проемов – при контроле защищенности от речевой разведки с использованием оптико-электронных средств разведки.

Контроль выполнения норм противодействия речевой разведке с применением оптико-электронных средств необходимо проводить путем вибрационных измерений на различных участках полотна оконного остекления по рекомендованным схемам. Количество контрольных точек в этом

случае определяется на каждом полотне остекления его площадью. При двойном остеклении без использования жалюзи между стеклами вибрационные измерения необходимо проводить как на внешнем, так и на внутреннем остеклении.

В процессе испытаний измерительный микрофон должен быть расположен на средней вертикальной линии на расстоянии от 1 до 2 м от внешней поверхности измеряемой ограждающей конструкции или ее участка и направлен в сторону конструкции.

Если ограждающая конструкция имеет выступающие элементы фасада, то микрофон должен быть размещен на расстоянии 1 м от вертикальной плоскости, проходящей через наиболее выступающие точки этих элементов фасада посредине ограждающей конструкции.

Защищенность речевой информации от ее перехвата по электронно-оптическому каналу аппаратурой технической разведки считается обеспеченной, если значение контролируемого параметра, рассчитанного по результатам вибрационных измерений на полотнах оконного остекления, не превышает нормированного значения.

Контрольные точки во время проведения контроля выполнения норм противодействия перехвату речевой информации по каналу непреднамеренного прослушивания (за счет слабой звукоизоляции ограждающих конструкций, звуковых каналов систем вентиляции и кондиционирования) выбираются на расстоянии 0,5 м от ограждающих конструкций на высоте 1, 5 м от пола с внешней стороны выделенного помещения.

Если технологические окна систем вентиляции и кондиционирования расположены на границе контролируемой зоны, то контролируемые точки выбираются непосредственно во входных (выходных) отверстиях воздуховодов систем вентиляции и кондиционирования.

Калибровка передающего измерительного комплекса

Перед проведением инструментальных измерений для получения достоверных результатов необходимо провести калибровку (градуировки) передающего измерительного комплекса. Суть калибровки состоит в установлении соответствия между положениями органов управления генератора шума совместно с усилителем мощности и интегральными уровнями звукового давления $L_к = L_н = 70$ дБ и $L_к = L_н + 20 = 90$ дБ, создаваемыми акустическим излучателем в свободном звуковом поле на расстоянии 1 м от его рабочего центра излучения.

Уровень звукового давления 90 дБ создается для превышения акустического (вибрационного) тестового сигнала в контрольной точке над акустическим (вибрационным) шумом в этой точке не менее чем на 3 дБ.

Уровень звукового давления 70 дБ используются при инструментальном контроле рабочих помещений, оборудованных системами звукоусиле-

ния. Номинальный выходной уровень звукового давления системы звукоусиления должен достигаться за счет изменения расстояния между акустическим излучателем передающего измерительного комплекса и микрофоном системы звукоусиления.

При проведении калибровки передающего измерительного комплекса акустический излучатель устанавливается на высоте 1,5 м от пола, а измерительный микрофон располагается на рабочей оси акустического излучателя на расстоянии 1 м от его рабочего центра.

Режим свободного поля обеспечивается при условии, когда в зоне радиусом 1,5 м от акустического излучателя и микрофона, отсутствуют ограждающие конструкции и предметы интерьера.

Размещение акустического излучателя передающего измерительного комплекса

Место установки акустического излучателя передающего измерительного комплекса в контролируемом помещении выбирается в зависимости от особенностей речевой деятельности в данном помещении.

В случае локализации источника речи в пределах конкретного рабочего места акустический излучатель следует устанавливать непосредственно на рабочем месте и ориентировать его по оси на контрольную точку, расположенную нормально к плоскости ограждающей конструкции.

Если в пределах рабочего помещения место источника речи конкретно не определено, то акустический излучатель необходимо размещать на высоте 1.5 м от пола и на расстоянии 1 м от вертикальной поверхности ограждающей конструкции. Ось излучателя ориентируется по нормали к обследуемой ограждающей конструкции. Аналогичные правила распространяются и на случаи обследования элементов инженерно-технических систем.

Если обследуемой конструкцией является пол или потолок, то акустический излучатель устанавливается в центре помещений на высоте 1,5 м от пола, и его направление излучения ориентируется по нормали к полу (потолку).

При контроле помещений, оборудованных системами звукоусиления, акустический излучатель передающего измерительного комплекса необходимо размещать у микрофонного входа системы на расстоянии, обеспечивающем номинальный режим работы системы звукоусиления.

Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, не оборудованных системой звукоусиления

Если защищаемое рабочее помещение не оборудовано системой звукоусиления, то установлен следующий порядок измерения отношений «сигнал/шум». В акустической системе передающего измерительного комплек-

са установливается уровень излучения 90 дБ. Для каждой выбранной контрольной точки с использованием приемного измерительного комплекса в каждой октавной полосе проводятся следующие измерительные и расчетные операции:

• при выключенном передающем измерительном комплексе измерить октавный уровень акустического (вибрационного) шума $L_{шi}$ ($V_{шi}$) в дБ;

• включить передающий измерительный комплекс и измерить октавный суммарный уровень (смесь) акустического сигнала и шума $L_{(с+ш)i}$ или вибрационного сигнала и шума $V_{(с+шi)}$;

• рассчитать октавный уровень акустического (вибрационного) сигнала $L_{ci}(V_{ci})$ по формулам

$$\begin{aligned} L_{сi} &= L_{(с+ш)i} - \Delta_1, \\ V_{сi} &= V_{(с+ш)i} - \Delta_1, \end{aligned} \qquad (6.11)$$

где Δ_1 – в дБ определяется из специальной таблицы.

• рассчитать октавное отношение «акустический (вибрационный) сигнал/шум» E_i в дБ по формулам

$$\begin{aligned} E_i &= L_{сi} - L_{шi} - 20, \\ E_i &= V_{сi} - V_{шi} - 20. \end{aligned} \qquad (6.12)$$

Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, оборудованных системой звукоусиления

При инструментальном контроле рабочих помещений, оборудованных системой звукоусиления, измерение отношений «сигнал/шум» производится в следующей последовательности.

Установить уровень излучения акустической системы 70 дБ и разместить ее перед микрофоном системы звукоусиления так, чтобы обеспечивался номинальный режим работы данной системы.

Для каждой выбранной контрольной точки с использованием приемного измерительного комплекса в каждой октавной полосе провести следующие измерительные и расчетные операции:

• при выключенном передающем измерительном комплексе измерить октавный уровень акустического (вибрационного) шума $L_{шi}$ ($V_{шi}$) в дБ;

• включить передающий измерительный комплекс и измерить октавный суммарный уровень (смесь) акустического сигнала и шума $L_{(с+ш)i}$ или вибрационного сигнала и шума $V_{(с+шi)}$;

• рассчитать октавный уровень акустического (вибрационного) сигнала L_{ci} (V_{ci}) по формулам:

$$\begin{aligned} L_{сi} &= L_{(с+ш)i} - \Delta_1, \\ V_{сi} &= V_{(с+ш)i} - \Delta_1, \end{aligned} \qquad (6.13)$$

где Δ_1 – в дБ определяется из соответствующей таблицы;

• рассчитать октавное отношение «акустический (вибрационный) сигнал/шум» E_i по формулам:

$$E_i = L_{\text{с}i} - L_{\text{ш}i} - 20,$$
$$E_i = V_{\text{с}i} - V_{\text{ш}i} - 20. \qquad (6.14)$$

Погрешность измерений должна оцениваться статистическими методами. Повторяемость результатов должна соответствовать данным, приведенным в нормативных документах.

Результаты инструментального контроля должны быть оформлены протоколом, а также рекомендациями и предложениями по обеспечению выполнения норм противодействия акустической речевой разведке.

6.6.4. Контроль технических средств и систем на соответствие установленным нормам на параметры в речевом диапазоне частот

1. Подготовительный этап контроля

На подготовительном этапе проводится:

• определение мест размещения ОТСС и ВТСС (с привязкой к помещениям, в которых они установлены) относительно трасс прокладки информационных и неинформационных цепей, выходящих за пределы контролируемой территории;

• проверка наличия проведения спецпроверок и специсследований ОТСС и ВТСС, а также выполнения требований предписаний на эксплуатацию этих средств;

• проверка наличия и правильности установки сертифицированных средств защиты информации по слаботочным и сильноточным цепям;

• проверка правильности прокладки (допустимые величины разноса) информационных и неинформационных токопроводящих цепей и коммуникаций в соответствии с требованиями СТР.

Опасными и подлежащими обязательному контролю являются все токопроводящие коммуникации и посторонние проводники (сети связи и передачи данных, электропитания, заземления, пожарно-охранной сигнализации, часофикации, радиофикации, инженерные коммуникации: водопровод, отопление и т.п.), имеющие выход за границу контролируемой зоны.

При отсутствии предписаний на эксплуатацию и заключений о специальной проверке технических средств аттестация объекта приостанавливается до выполнения необходимых мероприятий.

Проверка производится на основе следующих документов, входящих в паспорт объекта информатизации:

• план контролируемой зоны предприятия (учреждения);

• состав технических средств, расположенных в выделенном помещении;

• планы размещения основных и вспомогательных технических средств и систем в помещении;

• схемы прокладки линий передачи данных (слаботочные сети: телефон, пожарно-охранная сигнализация, часофикация, радиофикация и др.);

• схемы и характеристики систем электропитания и заземления объекта информатизации.

Проверка проводится в два этапа: сначала производится оценка правильности выполнения требований СТР по схемам, затем проверяется соответствие схем реальному размещению технических средств и прокладке линий.

2. Методика контроля

Контролю технических средств и систем с целью установления их соответствия нормам на параметры в речевом диапазоне частот соответствуют следующие технические мероприятия:

• инструментальная проверка уровня акустоэлектрических преобразований в ВТСС, подключенных к сетям и линиям, имеющим выход за границу контролируемой зоны;

• инструментальная проверка в ОТСС наличия паразитной генерации и наводок в линии электропитания.

Проверка паразитной генерации производится только на выявление факта наличия или отсутствия. В качестве измерительных приборов применяются анализатор спектр и осциллограф. Наличие модуляции проверяется по изменению уровня или изменению формы сигнала электромагнитного поля.

В случае выявления наличия паразитных генераторов, модулированных акустическим сигналом, техническое средство должно изыматься из выделенного помещения.

В качестве источника акустического сигнала используется генератор шума с интегральным уровнем звукового давления 70 дБ. Можно использовать генератор гармонического сигнала с частотой 1 кГц с перестройкой частоты на 10–15% в обе стороны для исключения резонансов. Измерения проводятся нановольтметром, имеющим шкалу 1 мкВ.

При установке несертифицированных или с просроченным сертификатом средств защиты производится обязательная проверка их работоспособности.

При выявлении нарушений требований СТР по допустимым величин разноса информационных и неинформационных токопроводящих цепей и коммуникаций допускается проведение инструментального контроля наличия наведенных электрических сигналов в отходящих цепях по методикам специальных исследований. Указанные проверки проводятся дополнительно к программе аттестационных испытаний.

В случае выявления превышения уровня сигнала установленных норм аттестационная проверка приостанавливается до устранения нарушений.

Вопросы для самопроверки

1. Что понимают под аттестационной проверкой?
2. Сущность контроля эффективности защиты информации.
3. Определение показателя эффективности защиты информации.
4. Что понимают под нормами эффективности защиты информации?
5. Что понимают под методом контроля эффективности защиты информации?
6. Виды методов технического контроля.
7. Цель и сущность технического контроля эффективности защиты информации.
8. Виды контроля эффективности защиты информации.
9. Каким может быть технический контроль эффективности технической защиты информации по характеру проведения и содержанию?
10. Средство контроля эффективности защиты информации (определение).
11. Необходимые условия для проведения технического контроля.
12. Виды контролируемых нормативных показателей.
13. Задачи контроля защищенности объекта от утечки по ПЭМИ.
14. В каком случае устройство объекта и сам объект считаются защищенными от утечки по ПЭМИ?
15. Виды контроля защищенности объектов от разведки по ПЭМИН.
16. Какой орган определяет состав нормативной и методической документации для аттестации конкретных объектов информатизации?
17. Состав нормативной и методической документации на методы испытаний.
18. Содержание технического контроля ЭВМ.
19. Порядок инструментального контроля ПЭМИН.
20. Задачи эксплуатационного контроля защищенности от утечки по ПЭМИН.
21. Содержание инструментальной части эксплуатационного контроля.
22. Каким должно быть значение напряжения (напряженности поля) посторонних радиопомех на каждой частоте измерений по ПЭМИН?
23. В каком случае допускается проведение испытаний в неэкранированном помещении?
24. Назначение поворотной платформы при измерениях напряженности поля ПЭМИН.
25. Структура систем защиты средств и систем информатизации от несанкционированного доступа.
26. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.

27. По какому признаку делается вывод о наличии акустоэлектрических преобразований ВТСС?

28. Если акустоэлектрические преобразования обнаружены, то каким образом можно оценить их опасность?

29. Цель проведения технического контроля акустической защищенности выделенного помещения.

30. Относительно каких мест проводится технический контроль акустической защищенности выделенного помещения?

31. Относительно каких мест проводится контроль защищенности от случайного (непреднамеренного) прослушивания?

32. Какие возможные технические каналы утечки учитываются при оценке мероприятий по информационной защите помещений?

33. Что предполагает инструментальный контроль акустической защищенности выделенных помещений?

34. При проведении контроля по информационной защите помещений какие основные исходные данные и документация проверяются?

35. Каким образом проводится технический контроль защищаемого помещения?

36. Что предполагает инструментальный контроль защищаемого помещения?

37. Содержание подготовительного этапа контроля защищенности выделенного помещения от утечки речевой информации.

38. Место съема информации для направленных микрофонов.

39. Способы контроля лазерного съема информации.

40. Для каких стекол проводится оценка при косвенном способе контроля лазерного съема информации?

41. По какому каналу проводится оценка защищенности акустической информации от случайного прослушивания?

42. Что является контролируемым параметром при контроле выполнения норм противодействия акустической речевой разведке в случае применения специальных автоматизированных комплексов?

43. Какой сигнал необходимо использовать в качестве тестового при акустическом инструментальном контроле?

44. Допустимо ли использовать в качестве тестового при инструментальном акустическом контроле гармонический сигнал?

45. Какие системы должны быть созданы для проведения инструментального контроля выполнения норм противодействия акустической речевой разведке при отсутствии автоматизированных комплексов?

46. Состав передающей измерительной системы контроля выполнения норм противодействия акустической речевой разведке.

47. Состав приемной измерительной системы контроля выполнения норм противодействия акустической речевой разведке.

48. Общие требования выбора контрольных точек при проверке выполнения норм противодействия акустической речевой разведке с применением микрофонов.

49. Общие требования выбора контрольных точек для вибрационных измерений при проверке выполнения норм противодействия акустической речевой разведке, если граница контролируемой зоны проходит по ограждающим конструкциям выделенного помещения.

50. Как выполняются акустические измерения в случае неоднородности ограждающей конструкции?

51. Место установки акустического излучателя передающего измерительного комплекса в контролируемом помещении в случае, если место источника речи конкретно не определено.

52. Место установки акустического излучателя передающего измерительного комплекса в контролируемом помещении в случае, если обследуемой конструкцией является пол или потолок.

7. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

7.1. Общие сведения

Под объектом информатизации, аттестуемым по требованиям безопасности информации, понимают совокупность информационных ресурсов, средств и систем обработки информации (автоматизированные системы различного уровня и назначения), используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, и выделенные помещения. Выделенное помещение – это специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

К нормативно-техническим документам относятся Нормы противодействия акустической речевой разведке (предельные возможности инженерно-технической разведки по добыванию информации), Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от ее утечки по техническим каналам (СТР), а также нормы и требования по защите информации от утечки по каналу ПЭМИН.

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в «Аттестате соответствия».

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

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

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. Государственную тайну составляют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

В некоторых случаях обработки конфиденциальной информации аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Сведения конфиденциального характера – сведения, входящие в следующий перечень:

– сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, составляющие тайну следствия и судопроизводства;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Состав видов технической разведки и их возможности, угрозы безопасности информации и каналы ее утечки, подлежащие контролю, определяются ФСТЭК России в соответствующих моделях технических разведок и концепциях защиты.

Технический контроль осуществляется в соответствии с методиками контроля состояния технической защиты информации, утвержденными или согласованными с ФСТЭК России.

Не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на

образцах, средствах и информационных системах в процессе выполнения ими обработки информации или технологического процесса.

Оценка разведдоступности

При оценке защиты информации различного уровня конфиденциальности, циркулирующей на объектах информатизации (ОИ) той или иной организации, всегда акцентируется внимание на типе защищаемой информации (речевая, документальная или цифровая) и физическом расположении центров ее циркуляции (выделенные помещения или автоматизированные системы).

После оценки оптимальности расположения ОИ решаются следующие вопросы: по каким каналам информация может покидать пределы ОИ, как и в каких объемах необходимо защищать эти каналы от утечки и соответствует ли защита предъявляемым или разрабатываемым самостоятельно критериям безопасности – соответственно разведдоступность, защищенность и аттестация.

Оценка разведдоступности включает в себя проверку возможности утечек информации по техническим каналам, проверку системы разграничения доступа физических лиц к конфиденциальной информации согласно их допуска и проверки режимности работы сотрудников (соответствия доступа к информации его допуску).

Проверка возможности утечки информации по техническим каналам состоит из комплекса следующих работ:

- Специальная проверка (СП) – проверка технических средств и систем объекта защиты с целью выявления специально установленных закладных устройств.

СП помещений проводится в первую очередь с помощью визуального осмотра, при котором тщательно изучаются коммуникации, строительные конструкции, мебель, канцелярские принадлежности, сувениры и другие объекты. В случае невозможности визуального доступа применяется специальная аппаратура для исследования внутреннего содержания обследуемых объектов. СП техники проводится путем демонтажа, визуального осмотра и рентгенографии.

Специалисты, проводящие такой осмотр, знакомы с внутренним устройством изучаемого технического оборудования и визуально способны определить изменения, привнесенные в конкретный объект, несмотря на то, что устройств, предназначенных для шпионажа или имеющих возможность использования в данном направлении, имеется большое множество.

- Специальные обследования выделенных помещений. Специальные обследования представляют собой комплекс мероприятий по выявлению возможно внедренных в ограждающие конструкции, предметы интерьера и другие места устройств съема информации. Проводятся с применением технических средств.

Специальные исследования (СИ) выделенных помещений на возможность утечки информации по акустическому и виброакустическому каналам

Специальные исследования предполагают выявление с помощью контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и оценку соответствия уровня защиты информации требованиям нормативных документов.

Данный вид СИ проводится для выделенных помещений с применением специального оборудования, по показаниям которого производится расчет ограждающих выделенное помещение конструкций на акустическую и вибрационную проницаемость.

Специальные исследования основных технических средств и систем на возможность утечки информации за счет побочного электромагнитного излучения и наводок (ПЭМИН)

В этом комплексе СИ производятся измерения технических средств на их возможность передачи информативного электромагнитного сигнала в пространстве и через коммуникации, а по полученным данным – расчет радиуса возможного съема этого сигнала.

Специальные исследования технических средств, входящих в состав ОИ, на возможность утечки информации за счет акустоэлектрических преобразований и высокочастотного навязывания

Данный вид СИ проводится для установления нерегламентированных возможностей технических средств преобразовывать акустический сигнал в электрический и передачу этого сигнала по линиям коммуникаций.

Испытания ОИ на наличие программных закладок и возможность несанкционированного доступа к защищаемой информации

Проверка разграничения доступа и режима работы проводится по разработанной для каждой отдельной организации документации, системе приказов, распоряжений и должностных инструкций, касающихся деятельности всех сотрудников организации.

По результатам проведенных работ производятся расчеты радиусов возможного съема информации напрямую или через систему коммуникаций связывающих организацию с внешним миром, и радиусов необходимых для соответствия необходимому уровню безопасности. Из сравнения данных показателей делается вывод о разведдоступности исследуемого ОИ и разрабатывается проект системы его защиты, включающий в себя рекомендации по изменениям и дополнениям в документации, регламентирующих работу с конфиденциальной информацией, и комплекса средств защиты информации (СЗИ), «закрывающих» все каналы, через которые возможна утечка информации.

Защищенность объекта информатизации

После выполнения всех рекомендаций и исполнения комплекса средств защиты информации (СЗИ), обеспечивающих защиту ОИ от воз-

можных утечек по техническим каналам и несанкционированного доступа, проводятся работы, аналогичные оценке разведдоступности ОИ, после которых следует расчет эффективности работы принятых мер по защите информации от ее утечки. Согласно результатам проведенных расчетов делается вывод о защищенности ОИ.

Аттестация объекта информатизации

Аттестация ОИ является заключительным этапом работ по защите информации, в который входит оценка требований, предъявляемых для исследуемых объектов информатизации организации заказчика и соответствие этим требованиям аттестуемых объектов. Результатом данной работы является аттестат соответствия, дающий право аттестующейся организации работать на своих ОИ с конфиденциальной информацией или как минимум уверенность в ее защищенности.

Аттестат выделенного помещения – документ, выдаваемый органом по аттестации (сертификации) или другим специально уполномоченным органом, подтверждающий наличие необходимых условий, обеспечивающих надежную акустическую защищенность выделенного помещения в соответствии с установленными нормами и правилами.

7.2. Мероприятия по выявлению и оценке свойств каналов утечки информации

Подробно и конкретно комплекс вопросов по выявлению каналов утечки информации рассмотрен в [38]. Краткое изложение и основные положения приведенного ниже материала соответствуют этому источнику.

Наличие каналов утечки информации определяется физическими свойствами среды распространения сигналов и характеристиками источников информации. Каналы утечки информации на объектах существуют всегда, но опасность они представляют только тогда, когда их информационные сигналы могут быть зафиксированы за пределами контролируемой зоны и расшифрованы. Для безопасности информации необходимо, чтобы уровень сигналов в каналах утечки был ниже воспринимаемого средствами технической разведки или же позволял маскирование сигналов. Сказанное не относится к информационным каналам с шифрованием сигналов.

Безопасный уровень сигналов каналов утечки определяется возможностями средств технической разведки. Так как средства технической разведки постоянно совершенствуются, то безопасный уровень сигналов в каналах утечки постоянно снижается.

Для обоснованного выбора действий по нейтрализации каналов утечки информации необходимо их выявить, произвести оценку реальной угрозы утечки информации и выработать необходимый комплекс защитных мер.

Важное значение для оценки реальной угрозы утечки информации имеет определение уровня сигналов в каналах утечки.

Методики и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации определены нормативно-методическими документами. В документах приведен перечень работ по выявлению каналов утечки информации, который предусматривает:

- специальные проверки (СП);
- специальные обследования (СО);
- специальные исследования (СИ).

В свою очередь, специальные исследования объединяют в себе в общем случае следующие исследования:

- специальные исследования акустических и виброакустических каналов;
- специальные исследования побочных электромагнитных излучений и наводок устройств обработки информации;
- специальные исследования линий электропитания устройств обработки информации.

7.2.1. Специальные проверки

Специальные проверки представляют собой проверки технических средств и систем (ТСС) объекта защиты с целью выявления и изъятия специально установленных закладных устройств съема информации непосредственно с ТСС, выявление технических доработок по изменению свойств ТСС, облегчающих умышленный или неумышленный съем информации, выявление различного рода программных закладок съема информации. При проведении специальных проверок применяются специализированные технические средства.

Данный вид работ лицензируется, контролируется и проводится на основании нормативно-методических документов Службы специальной связи и информации при Федеральной службе охраны Российской Федерации.

Специальная проверка предшествует специальным исследованиям и состоит из нескольких последовательно выполняемых действий [38]:

- прием-передача проверяемого технического средства представителям исследовательских лабораторий или сертификационных центров, формирование исходных данных для программы проверки;
- составление программы проведения специальной проверки технического средства;
- проведение проверки;
- анализ результатов проверки, составление отчетных протоколов.

На специальную проверку технические средства должны предъявляться в исправном состоянии, в штатной упаковке и в полной комплектации по акту приема-передачи. Акт приема-передачи подписывается только по-

сле проверки работоспособности технического средства. В случае неисправности технического средства специальная проверка не производится.

Кроме технического средства, представители организации, которой оно принадлежит, обязаны предоставить для разработки программы проверки информацию следующего вида:

- данные о техническом средстве;
- сведения о его планируемом применении;
- данные о месте размещения технического средства.

Данные о техническом средстве должны содержать сведения о его назначении и полной комплектации, комплект документов на техническое средство, способ приобретения с указанием сведений об организации-поставщике.

Данные о планируемом применении должны содержать сведения:

- планируется ли техническое средство для обработки закрытой информации;
- есть ли высший гриф секретности у обрабатываемой или обсуждаемой информации;
- в составе какой информационной системы планируется работа технического средства;
- к каким коммуникационным системам планируется подключение технического средства.

Сведения о планируемом размещении технического средства должны содержать:

- описание объекта информатизации, на котором планируется использовать техническое средство;
- перечень охраняемых сведений объекта информатизации;
- минимальное расстояние до границы контролируемой зоны;
- наличие посольств, представительств и мест пребывания иностранных граждан с указанием расстояния до контролируемой зоны;
- возможность и периодичность пребывания иностранных делегаций на объекте.

Программа проведения специальной проверки должна учитывать, что возможно установленные электронные закладные устройства или программные закладки ориентированы на получение вполне конкретной информации или на выведение из строя технических средств обработки информации.

По имеющимся документам проводится анализ схемотехнических особенностей электронного технического средства и источника его питания с целью выявления мест циркуляции обрабатываемой информации.

Итогом анализа исходных данных, схемотехнических особенностей и иных необходимых сведений с учетом классификации электронного уст-

ройства должен явиться перечень каналов утечки информации и возможно внедренных аппаратных закладных устройств.

Далее на основании перечня естественных каналов утечки информации и возможно внедренных закладных устройств составляется программа проведения специальной проверки технического средства, определяющая порядок выявления демаскирующих признаков закладного устройства и самого устройства. Результаты оформляются в журнале проведения специальных проверок и заверяются подписью руководителя рабочей группы.

Типовой перечень операций проведения специальных технических проверок состоит из [38]:

- дозиметрического контроля изделия в упаковке для обнаружения радиоактивных меток и радиоизотопных источников питания;
- вихретокового контроля узлов технических средств обработки информации, не содержащих металлических включений;
- контроля упаковки, которая по назначению не должна иметь полупроводниковых приборов, нелинейным локатором для выявления специального электронного устройства, выполняющего роль маяка для определения местоположения технического средства;
- проведения радиоконтроля для выявления активных закладных устройств передачи информации по радиоканалу;
- проверки возможности съема информации методом высокочастотного навязывания;
- разборки технического средства с последующим осмотром его узлов для выявления отклонения от схемотехнических и конструкторских решений;
- измерений импедансов некоторых узлов технических средств для выявления их отклонений от нормы из-за возможно внедренных аппаратных закладок;
- рентгенографии или рентгеноскопии неразборных узлов и элементов технических средств с целью выявления схемных изменений;
- рентгенотелевизионного и визуально-оптического контроля внешнего вида и внутренней структуры узлов и элементов технических средств.

Сложные виды контроля (визуально-оптический контроль, рентгеновский контроль, контроль методами нелинейной локации, электротехнических измерений и высокочастотного «навязывания») проводятся по специальным методикам.

Проверенные технические средства и оборудование маркируются по специальной методике.

По результатам проведения специальной проверки руководитель проверяющей группы делает вывод о наличии или отсутствии закладных электронных устройств и оформляет акт с перечислением проверенных элементов, видов технических проверок и фамилий и инициалов проводивших отдельные виды проверок лиц. Акт оформляется в единственном экземпля-

ре и хранится у исполнителя. Заключение составляется в двух экземплярах (для исполнителя и заказчика). Акт и заключение утверждаются руководителем организации-исполнителя.

7.2.2. Специальные обследования

Подготовительные работы

Под специальными обследованиями выделенных помещений понимают комплекс мероприятий по выявлению возможно установленных электронных устройств съема информации в ограждающих конструкциях, предметах интерьера, бытовых приборах и проводных коммуникациях выделенного помещения. Специальные обследования, как правило, проводятся с применением специальных технических средств.

Специальные обследования выделенных помещений проводятся в форме поисковой операции под видом ремонтно-строительных работ для отвлечения внимания вероятного противника, заинтересованного в получении информации ограниченного пользования.

До проведения поисковой операции вероятный противник чаще всего неизвестен, поэтому построение его модели часто приходится проводить со слов заявителя. Если заявитель отмечает сбои в работе телефонной связи или иные косвенные признаки незаконных попыток получения конфиденциальной информации, то в этом случае вполне вероятна организация противником каналов утечки на профессиональном уровне. Профессиональная организация каналов утечки информации требует значительных финансовых затрат, причем чем выше уровень профессионализма, тем больше затраты и выше сложность методов и средств добывания информации противником. Это обстоятельство необходимо учитывать при построении модели вероятного противника и оценке характера его действий.

После создания модели противника производится оценка условий выполнения поставленной задачи [38]:

- изучается расположение на местности объекта и окружающей территории с имеющимися на ней другими объектами;
- определяется возможность съема информации из-за пределов контролируемой зоны;
- обследуется сам объект с составлением планов помещений с нанесенными входящими и выходящими коммуникациями.

При обследовании объекта в первую очередь выясняют:

- взаимное расположение контролируемых и смежных помещений, порядок их посещений;
- факты и сроки проведения ремонтных работ и монтажа (демонтажа) коммуникаций, даты замены предметов интерьера;

• конструктивные особенности ограждающих конструкций, материалы покрытий.

Особое внимание должно быть уделено прилегающей к контролируемой зоне территории, которая может быть использована в качестве парковки автомобилей с различного рода разведывательной аппаратурой дистанционного действия.

Основываясь на модели возможного противника и сведениях об объекте, планируют виды и объем поисковых действий, перечень контрольно-измерительной аппаратуры, состав специалистов и подсобных рабочих, сроки проведения работы. К выполнению работ могут быть допущены по согласованию работники заказывающей организации.

Тщательному анализу на уязвимость должны быть подвержены проводные коммуникации (силовая и телефонная сети, сигнализация), выходящие за пределы контролируемой зоны. Проводные коммуникации могут служить каналом передачи сигналов от линейных закладок, а телефонные линии – источником речевой и цифровой (при работе факса) информации.

Проверка коммуникаций выполняется с участием специалистов, их эксплуатирующих.

После предварительного анализа обстановки руководитель поисковой группы должен иметь комплект документов [38]:

• согласованную с заказчиком отвлекающую причину проведения поисковых работ;

• план прилегающей территории с указанием назначения строений;

• поэтажный план здания, в котором расположен объект, с обозначением смежных и выделенного помещений;

• сведения об организациях или частных лицах, работающих в смежных помещениях;

• протокол с характеристиками ограждающих конструкций и материалов их покрытий;

• схему сооружений жизнеобеспечения с привязкой к плану выделенного помещения;

• схему входящих и выходящих проводных коммуникаций;

• план размещения предметов интерьера в помещении;

• план-график работ с указанием ответственных исполнителей;

• перечень необходимой для работы исследовательской аппаратуры.

Выполнение поисковых мероприятий

Поисковые мероприятия на объекте в наиболее распространенном случае состоя:

• из радиообнаружения;

• из осмотра помещения;

• из обследования электрических и электронных приборов;

• из проверки проводных коммуникаций.

Для выполнения мероприятий необходимы металлодетекторы, индикаторы электромагнитного поля, нелинейные локаторы, сканирующие приемники и радиочастотомеры, анализаторы спектра, переносные рентгеновские и тепловизионные приборы, программно-аппаратные комплексы для проведения радиомониторинга и другие необходимые по обстоятельствам средства.

Радиообнаружение. Для достоверного обнаружения радиозакладных устройств желательно иметь карту загрузки радиочастотного диапазона на расстоянии от 300 до 1000 м от объекта (вне зоны действия радиозакладного устройства). Это упрощает обнаружение закладки в ближней зоне ее действия, если провести сравнительный анализ радиочастотного диапазона непосредственно на объекте и в удаленной точке, отбросив сигналы известных станций и нелегальных источников излучений.

Современные программно-аппаратные комплексы (например, RS turbo) за счет зондирующего акустического сигнала позволяют проводить обнаружение и локализацию сравнительно простых радиозакладных устройств с постоянной несущей частотой и передачей по открытому каналу. Несмотря на небольшую вероятность применения такие радиозакладные устройства исключать из рассмотрения нельзя.

Радиозакладные устройства постоянно совершенствуются, а производство аппаратуры для их обнаружения отстает от потребности. Арсенал закладочных устройств стремительно пополняется новыми высокотехнологичными изделиями с высокой скрытностью работы от традиционных средств обнаружения сигналов. В закладных устройствах все чаще применяются различные способы накопления информации, позволяющие резко сократить время ее передачи или отложить передачу на другое, более удобное время. В этих устройствах все шире используются разнообразные методы закрытия информации, шумоподобные широкополосные сигналы, работа в занятых каналах, специальные алгоритмы скачкообразной перестройки несущей частоты, полуактивный режим работы и другие приемы. Это определяет высокие требования к квалификации операторов.

Универсальными методами обнаружения радиозакладных устройств являются сравнительный радиоконтроль и энергетическая локализация с помощью индикаторов электромагнитного поля.

Применяемое оборудование: комплекс радиоконтроля, который позволяет обнаружить и локализовать микрорадиопередатчики, составить карты загрузки радиоэфира (базы данных принятых радиосигналов и их характеристик). Эти карты послужат исходным материалом при проведении последующих проверок на объекте.

Осмотр помещения. Осмотр помещения подразделяется на первичный осмотр и техническую проверку [38].

Первичный осмотр проводится как визуальный контроль помещения и находящихся в нем предметов. Если имеется план или фотографии, то производят сверку фактического размещения предметов с документально зафиксированным. Электронные приборы временно удаляют или размещают в определенном месте. Мебель отодвигают от стен и осматривают содержимое ящиков. Регистрируют наименования предметов, серийные номера, номера печатей и пломб.

Осматривая стены и потолок, обращают внимание на крепления плиток, наличия на них царапин, на наличие посторонних предметов в межпотолочном пространстве.

Осветительные приборы снимают, разбирают и осматривают. Обследуют ниши и подводящие провода электророзеток.

С помощью эндоскопов и осмотровых зеркал обследуют вентиляционные короба.

В местах установки отопительных батарей обследуют ниши, места ввода труб в стены, межсекционные пространства.

Проверяют также предметы, находящиеся на стенах, мебель, складки обивки мягкой мебели, сувениры, игрушки и т.п.

Все подозрительные предметы откладывают в отдельное место для последующей проверки.

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

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

Наиболее информативными признаками проводной микрофонной системы являются:

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

Демаскирующие признаки автономных некамуфлированных акустических закладок включают:

- признаки внешнего вида – малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
- одно или несколько отверстий малого диаметра в корпусе;
- наличие автономных источников питания (например, аккумуляторных батарей);
- наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;

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

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

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

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

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

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

Дополнительные демаскирующие признаки акустических радиозакладок:

• радиоизлучения (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сигналом;

• наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.

Вследствие того, что при поиске радиозакладок последние находятся в ближней зоне излучения и уровень сигналов от 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 «∞» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

• отличие сопротивления телефонной линии от типового значения (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии на распределительной коробке (щитке);

• падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;

• наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне.

Дополнительные демаскирующие признаки акустических закладок типа «телефонного уха»:

• отличие сопротивления телефонной линии от «∞» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

• падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной телефонной трубке;

• наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне;

• подавление (не прохождение) одного-двух вызывных звонков при наборе номера телефонного аппарата.

Дополнительные демаскирующие признаки полуактивных акустических радиозакладок:

• облучение помещения направленным (зондирующим) мощным излучением (как правило, гармоническим);

• наличие в помещении переизлученного зондирующего излучения с амплитудной или частотной модуляцией информационным акустическим сигналом.

Наиболее информативными признаками проводной микрофонной системы являются:

- тонкий провод неизвестного назначения;
- наличие в линии неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного сигнала.

Признаками не камуфлируемых акустических закладок являются:

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

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

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

Дополнительные признаки акустических радиозакладок:

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

Демаскирующие признаки сетевых акустических закладок:

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

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

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

Дополнительные признаки телефонных радиозакладок:

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

Техническую проверку предметов мебели и интерьера проводят при помощи нелинейного локатора и портативного рентгеновского аппарата на подготовленной для этой цели площадке. После проверки подозрительные предметы желательно промаркировать специальными невидимыми при обычном освещении метками.

Опись предметов с планом их расположения передают представителю заказчика.

Последним этапом аппаратурной проверки является обследование ограждающих конструкций нелинейным локатором.

Сначала обследуют все смежные помещения, включая и расположенные на смежных этажах. При этом все электронные устройства внутри выделенного помещения необходимо убрать или отодвинуть от ограждающих поверхностей как можно дальше, так как зона действия нелинейного локатора может быть более 1 м. Для ускорения действий и повышения достоверности результатов обнаружения полупроводниковых устройств желательно использовать нелинейный локатор с индикацией второй и третьей гармоник переотраженного сигнала. По соотношению гармоник распознают коррозионные нелинейности и «чистые» полупроводники.

При первом проходе зондируют всю поверхность, отмечая места, где получены сигналы отклика. Для уточнения результатов зондирования нелинейный локатор переносят на другую сторону ограждающей конструкции и снова анализируют ситуацию в подозрительных местах. В подозрительных местах проводят рентгеноскопический анализ для получения окончательных выводов.

Эффективность и, следовательно, целесообразность установки противником электронных стетоскопов на хорошо проводящих звук конструкциях из твердых материалов проверяют измерительным электронным стетоскопом.

Проверка электрических и электронных приборов. Электрические приборы (настольные лампы, холодильники, электрические удлинители и т.п.) включают в сеть и индикатором электромагнитного поля проверяют наличие радиоизлучений. В подозрительных случаях прибор проверяют более совершенным измерительным комплексом с целью уточнения характеристик излучаемого сигнала, обесточивают, разбирают и осматривают.

Значительно сложнее выявить закладные устройства в электронных бытовых приборах и средствах оргтехники, которые сами являются источниками электромагнитных излучений. Поэтому их проверку проводят в специализированных лабораториях, хотя не исключается вариант проверки на месте путем сравнения печатных плат с размещенными компонентами электронной схемы с аналогичными платами от других приборов такого же типа. В процессе сравнения необходимо обращать внимание на наличие дополнительных компонентов схемы неизвестного назначения и подключенных к источнику питания. Особое внимание необходимо обращать на

изменение топологии печатной платы, так как внедрение закладки на плату неизбежно приведет к появлению дополнительных электрических соединений.

При осмотре электронных приборов необходимо также обращать внимание на изменение внешнего вида радиокомпонентов, наличие на них отверстий небольшого диаметра для микрофона.

Проверенные приборы опечатывают пломбами или маркируют ультрафиолетовыми метками.

Проверка проводных коммуникаций. Проверка проводных коммуникаций начинается с выяснения трасс прокладки каждой линии. Если имеется техническая документация на монтажные схемы, то ее используют в качестве источника первичной информации. Для уточнения трасс линий применяют трассо- и металлоискатели. Проверяются линии электроснабжения, телефонные линии, кабели сигнализации и коммутационные устройства (распределительные щиты, коробки и т.д.). Выясняют наличие посторонних проводников неизвестного назначения.

Линии проверяют на наличие модулированных высокочастотных сигналов, а слаботочные линии – на наличие информационных низкочастотных сигналов.

При проверке линий их отключают от распределительных щитков, подключают к локатору коммуникаций и нагружают на эквивалентное сопротивление. По результатам локации определяют наличие или отсутствие закладных устройств.

Применяемое оборудование: анализатор проводных линий, анализатор параметров телефонной линии, проводной приемник, усилитель НЧ-сигналов, комплект специальных инструментов и принадлежностей, контрольно-измерительные приборы (мегомметр, мультиметр).

После проведения специального обследования оформляются следующие отчетные документы [38]:

- протоколы с указанием мест реагирования измерительных приборов, участков вскрытия ограждающих конструкций, описанием подозрительных предметов мебели и интерьера;
- протоколы изъятия средств съема информации;
- заключение об уровне информационной защищенности объекта;
- рекомендации по перекрытию технических каналов утечки информации.

Документы согласовывают с заказчиком и передают в его службу безопасности.

7.2.3. Специальные исследования

Под специальными исследованиями согласно ГОСТ Р 51624-00 понимают выявление с использованием контрольно-измерительной аппаратуры

возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

Оценка соответствия защиты информации требованиям нормативных документов невозможна без объективных измерений уровня информационных сигналов в крайних точках канала утечки. В одних случаях определяется уровень сигналов утечки информации непосредственно у источника и расчетным путем производится его оценка на границе контролируемой зоны, в других случаях измерение сигналов утечки информации производится на границе контролируемой зоны, чем обеспечиваются более объективные результаты. Без такой оценки невозможно выявление каналов утечки информации – основной задачи специальных исследований.

Конечным результатом специальных исследований должно быть вычисление отношения сигнал/шум и сравнение полученного значения с нормированными значениями.

До проведения специальных исследований необходимо провести детальный анализ особенностей всех технических средств ОИ, составить список исследуемых устройств и помещений и в обязательном порядке результаты зафиксировать в протоколах в качестве обоснования выбора опасных каналов утечки информации. Эта работа проводится совместно заказчиком и исполнителем.

В большинстве случаев выявление возможных характеристик опасных сигналов производится в тестовых режимах работы технического средства. Тестовые режимы позволяют установить необходимый уровень и форму опасного сигнала и гарантированно его выделить при измерении на фоне других сигналов по известным признакам.

Измерение опасных сигналов должно в обязательном порядке проводиться только средствами измерений, внесенными в Госреестр средств измерений и имеющими не просроченное «Свидетельство о поверке». В некоторых случаях измерительные системы и комплексы должны иметь сертификат ФСТЭК России.

7.2.3.1. Специальные исследования акустических и виброакустических каналов

Специальные исследования в области акустики проводятся в основном применительно к выделенным помещениям (ВП). Исследуемыми объектами являются ограждающие помещение конструкции, все каналы, трубопроводы и другие проводящие звук инженерные конструкции.

В протоколе специальных исследований (СИ) в области акустики и виброакустики в [38] рекомендуется отразить:

• *название организации*, выполняющей СИ, ссылку на его лицензии и название объекта СИ;

• *объекты контроля* (ВП) и их краткое описание;

• *уровень защиты* для каждого из них (категория ВП);

• *размещение* ВП;

• *перечень граничащих с ВП помещений* во всех направлениях с приведением плана размещения по отношению к смежным помещениям;

• *перечень* ограждающих конструкций ВП.

Для ВП должны быть заранее известны границы контролируемых зон отдельно для акустических и виброакустических каналов. Должны быть также проанализированы особенности структуры ограждающих конструкций с целью выбора для исследований опасных участков, на которых возможна утечка акустической информации.

Действующая методика измерений акустических и виброакустических характеристик различных сред базируется на определении двух величин – звукового давления в воздушной среде и виброускорения на поверхности твердого тела [38]. Обе величины определяются специальными устройствами на основе шумомеров, на вход которых подаются сигналы от измерительных датчиков – микрофонов и акселерометров. Звуковые тест-сигналы формируются акустическими генераторами с регулируемыми по уровню и частотным характеристикам выходными акустическими сигналами.

В настоящее время достаточно широко применяются удобные шумомеры моделей фирмы RFT и отечественные аналоги серии ВШВ. Шумомеры должны быть поверены и числиться в Государственном реестре.

Микрофоны (в основном конденсаторные) и акселерометры пригодны любых моделей, если они имеют достаточную точность.

Дополнительно к указанным приборам необходим акустический калибратор в качестве эталона звукового давления для калибровки микрофонов.

Кроме комплектов измерительных приборов существуют программно-аппаратные комплексы для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическим и виброакустическим каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств, образованных за счет акустоэлектрических преобразований. Из таких комплексов наиболее известными являются «Трап», «Спрут», «Шепот» и «Гриф».

Комплекс «Трап» реализует методику измерения, отличающуюся от действующей, и может давать ошибки за счет интерференции в помещении тестового сигнала типа «плавный тон».

Комплексы «Спрут» и «Шепот» имеют высокую степень автоматизации вычислений в полном соответствии с утвержденной методикой.

Приведем краткую характеристику одного из программно-аппаратных комплексов акустических и виброакустических исследований – «Спрут-7».

Комплекс предназначен для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, а также за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств в речевом диапазоне частот, образованных за счет акустоэлектрических преобразований. Комплекс обеспечивает измерение характеристик акустических сигналов, в том числе октавный, треть октавный анализ и анализ с использованием функции быстрого преобразования Фурье (БПФ), проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления, измерение уровней сигналов акустоэлектрических преобразователей с использованием функции БПФ.

Программно-аппаратный комплекс «Спрут-7» состоит из трех подсистем:

– измерительной подсистемы;

– подсистемы источника тестового акустического сигнала;

– подсистемы управления.

Модуль источника тестового акустического сигнала «SZATG-03» генерирует следующие виды сигналов:

– непрерывный гармонический сигнал на частотах, соответствующих средним частотам третьоктавных полос в диапазоне от 20 до 20000 Гц;

– белый шум;

– розовый шум.

Специальное программное обеспечение (СПО) предназначено для управления измерительным модулем и модулем источника тестового акустического сигнала, получения результатов измерений, их обработки, отображения и сохранения в необходимом формате.

Внешний вид главного окна программы управления показан на рис. 7.1.

Главное окно программы имеет две основные области:

– панель измерительного модуля;

– панель источника тестового акустического сигнала.

На панели спектров могут быть одновременно отображены 2 спектра входного сигнала. Выбор этих спектров осуществляется пользователем, который определяет, что отображается в качестве спектра № 1 из перечня:

- усредненный спектр;
- накопление максимумов;
- накопление минимумов.

а что отображается в качестве спектра № 2 из перечня:

- текущий спектр;
- усредненный спектр;

- накопление максимумов;
- накопление минимумов;
- образец.

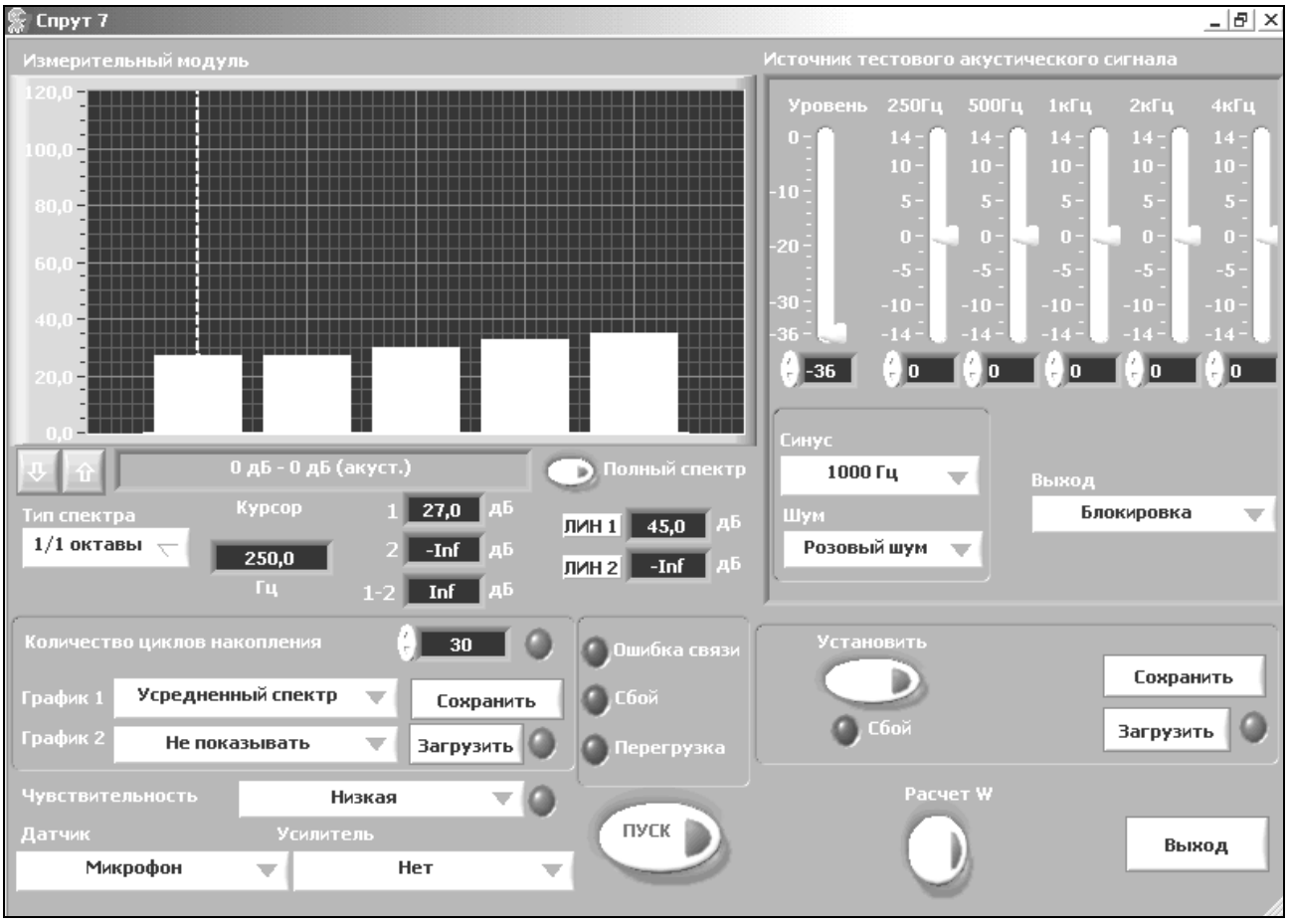


Рис. 7.1. Внешний вид главного окна СПО «СПРУТ-7»

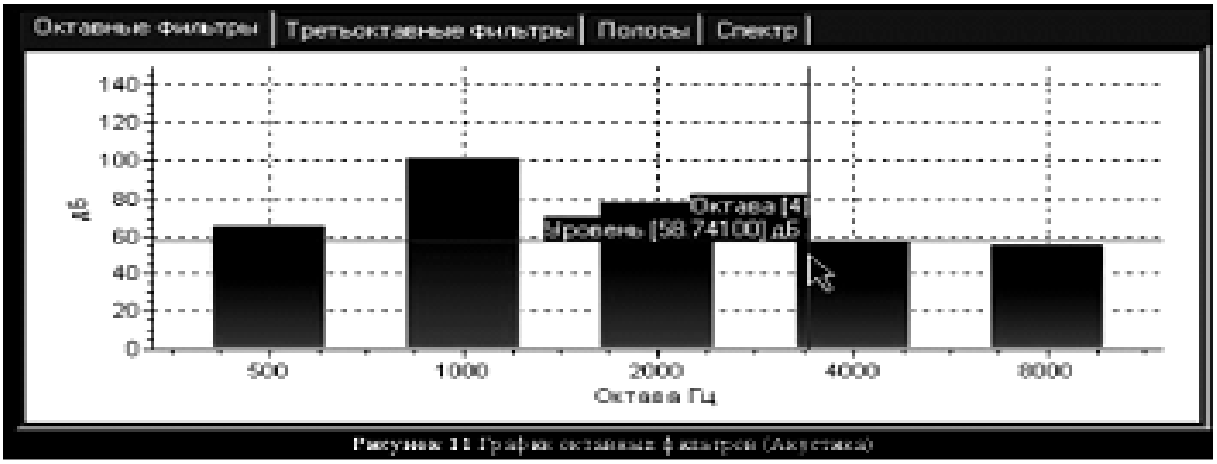
В качестве образца может быть загружен из файла сохраненный ранее спектр.

При работе с программой пользователю для анализа информации предоставляются графики, показанные на рис. 7.2. График октавных фильтров (*а*) отображает значения с использованием октавного фильтра с центральными частотами: 500 Гц, 1000 Гц, 2000 Гц, 4000 Гц, 8000 Гц. Значения отображаются в децибелах.

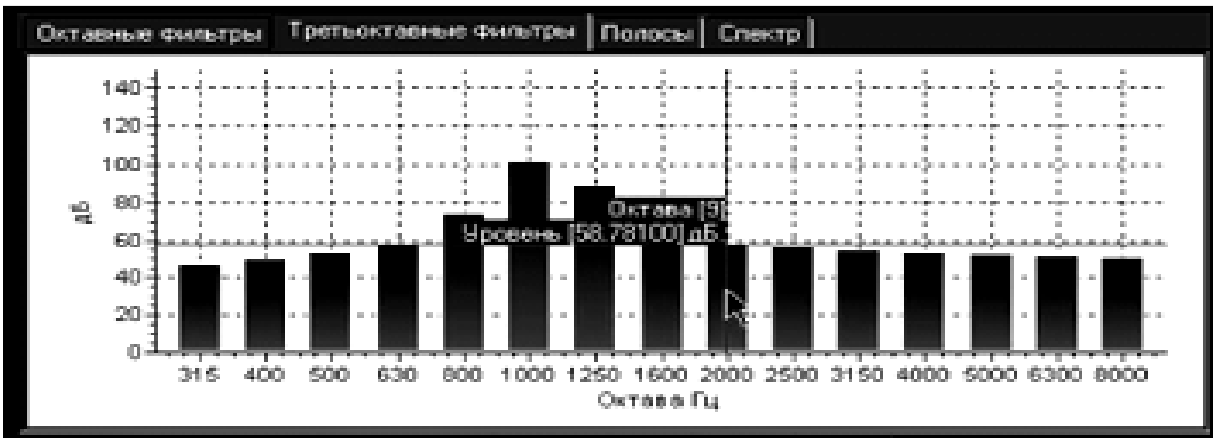
График третьоктавных фильтров (*б*) отображает значения с использованием третьокнавных фильтров с центральными частотами: 315 Гц, 400 Гц, 500 Гц, 630 Гц, 800 Гц, 1000 Гц,1250 Гц,1600 Гц, 2000 Гц, 2500 Гц, 3150 Гц, 4000 Гц, 5000 Гц, 6300 Гц, 8000 Гц. Значения отображаются в децибелах.

График полосных фильтров (*в*) отображает значения с использованием полос типа: Фильтр A, Фильтр B, Фильтр C, Фильтр D, Линейный фильтр. Значения измеряются соответственно в: дБA, дБB, дБC, дБD, дБLin.

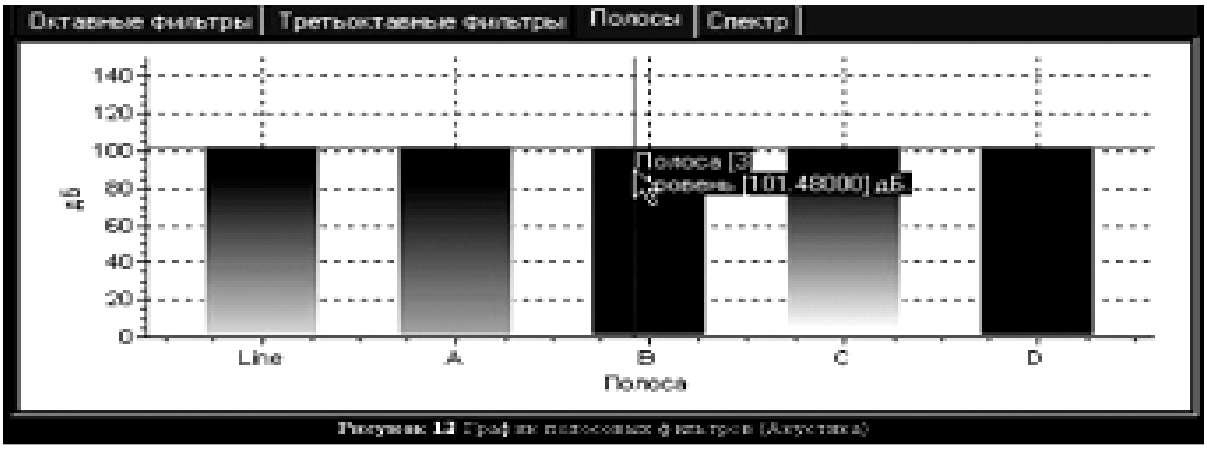
а



б



в



г

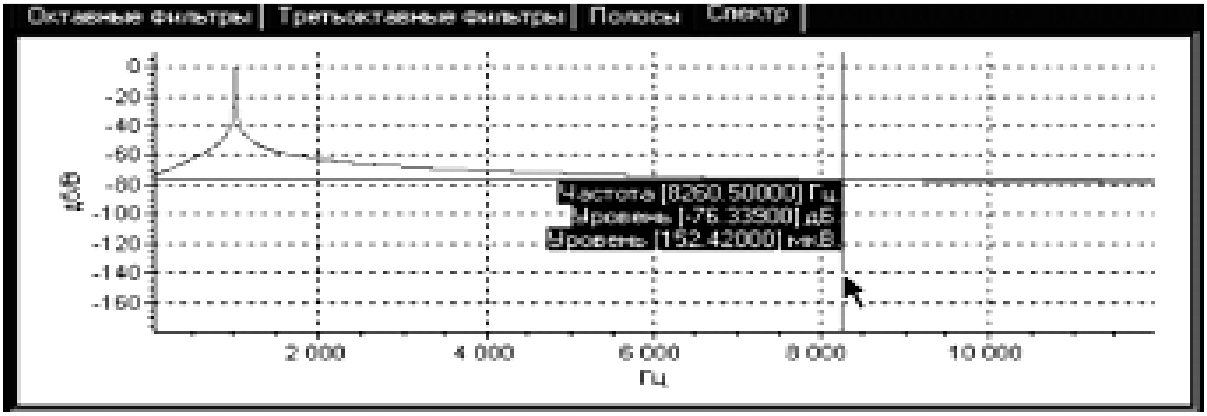


Рис. 7.2. Графики фильтров и спектра сигнала: *а* – октавных фильтров, *б* – третьоктавных фильтров, *в* – полосных фильтров, *г* – спектра сигнала

График спектра сигнала (*г*) отображает спектральную характеристику сигнала в диапазоне от 25 Гц до 12500 Гц. Значение спектральных составляющих отображаются в дБ/В и В (с перестраиваемым множителем).

Последним на рынке появился комплекс «Гриф». Так как данный комплекс не имеет расчетной программы для вычисления интегрального индекса артикуляции речи R и зависимости словесной разборчивости речи W от интегрального индекса артикуляции речи, то все вычисления производятся по методике, изложенной в [41].

Согласно методике спектр разбивается на N в общем случае произвольных частотных полос, но чаще всего октавных или третьоктавных. Для каждой i-й частотной полосы на каждой среднегеометрической частоте $f_{\text{ср}i} = \sqrt{f_{\text{в}i} f_{\text{н}i}}$ определяется формантный параметр ΔA_i, характеризующий энергетическую избыточность дискретной составляющей речевого сигнала:

$$\Delta A_i = L_{\text{с}i} - A_i, \text{ дБ}, \qquad (7.1)$$

где $L_{\text{с}i}$ – средний спектральный уровень речевого сигнала в контрольной точке для i-й спектральной полосы; A_i – средний спектральный модальный уровень формант в той же полосе.

Значение формантных параметров определяются по графику рис. 7.3 при условии $f = f_{\text{ср}\,i}$ или по формуле

$$\Delta A(f_{\text{ср}i}) = \begin{cases} 200/f^{0,43} - 0,37, & \text{если } f \le 1000 \text{ Гц}; \\ 1,37 + 1000/f^{0,69}, & \text{если } f > 1000 \text{ Гц}; \end{cases} \qquad (7.2)$$

где $\Delta A(f_{\text{ср}i}) = \Delta A_i$.

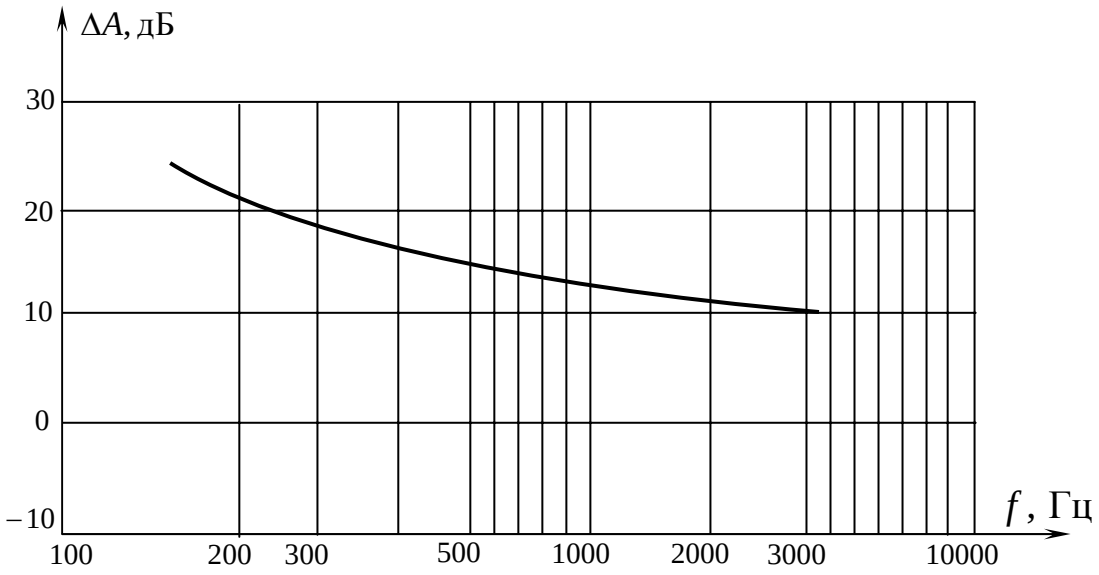


Рис. 7.3. Разница между спектральным уровнем речи и формант

Для каждой i-й частотной полосы определяется весовой коэффициент $k_i = k(f_{\text{в}i}) - k(f_{\text{н}i})$ как разность весовых коэффициентов для верхней и нижней граничных частот частотной полосы спектра речевого сигнала.

Весовой коэффициент k_i характеризует вероятность наличия формант речи в частотной полосе.

Весовые коэффициенты $k(f_{вi})$ и $k(f_{нi})$ находятся по кривой рис. 7.4 или рассчитываются по формулам

$$k(f)=\begin{cases}2{,}57\cdot10^{-8}\,f^{2,4}, & \text{если } 100<f<400 \text{ Гц};\\ 1-1{,}074\exp(-10^{-4}\cdot f^{1{,}18}), & \text{если } 400<f<10000 \text{ Гц};\end{cases} \tag{7.3}$$

если $f = f_{вi}$ и $f = f_{нi}$.

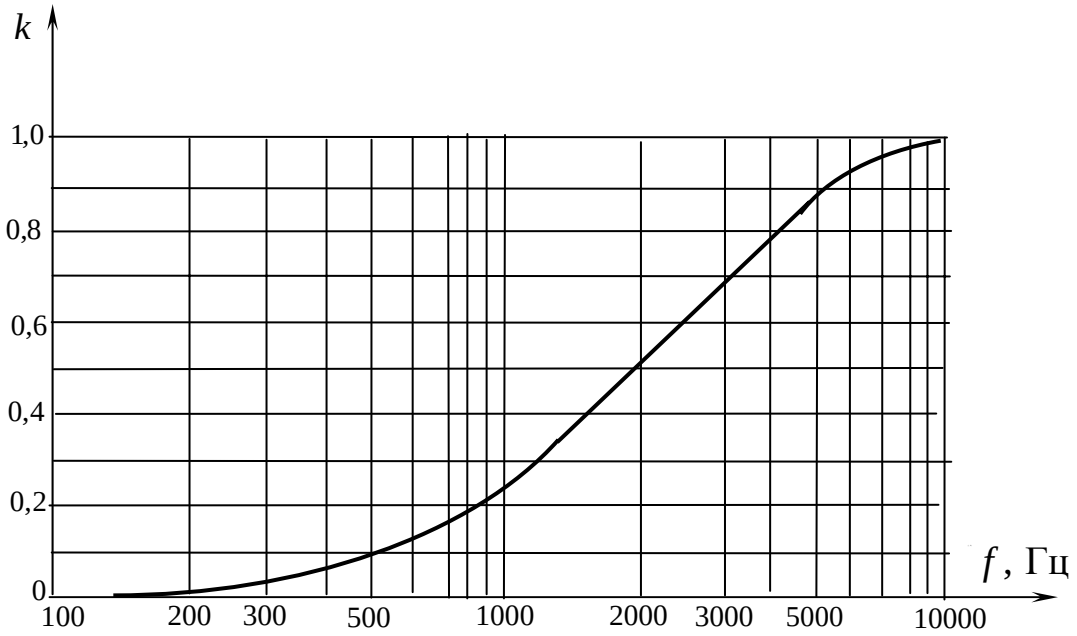


Рис. 7.4. Формантное распределение

На среднегеометрической частоте $f_{срi}$ для каждой частотной полосы по кривой рис. 7.5 или по формулам

$$p_i=\begin{cases}\dfrac{0{,}78+5{,}46\exp[-4{,}3\cdot10^{-3}(27{,}3-|Q_i|)^2]}{1+10^{0{,}1|Q_i|}}, & \text{если } Q_i\le 0;\\ 1-\dfrac{0{,}78+5{,}46\exp[-4{,}3\cdot10^{-3}(27{,}3-|Q_i|)^2]}{1+10^{0{,}1|Q_i|}}, & \text{если } Q_i>0\end{cases} \tag{7.4}$$

определяется коэффициент восприятия формант человеком p_i, характеризующий вероятное относительное количество формантных составляющих речи с уровнями интенсивности выше порогового значения.

В (7.4) приняты обозначения:

$Q_i = A_i - L_{шi} = q_i - \Delta A_i$ – относительный уровень интенсивности формант; $L_{шi}$ – уровень шума в i-й спектральной полосе; $q_i = L_{ci} - L_{шi}$ – отношение «уровень речевого сигнала/уровень шума» в i-й спектральной полосе.

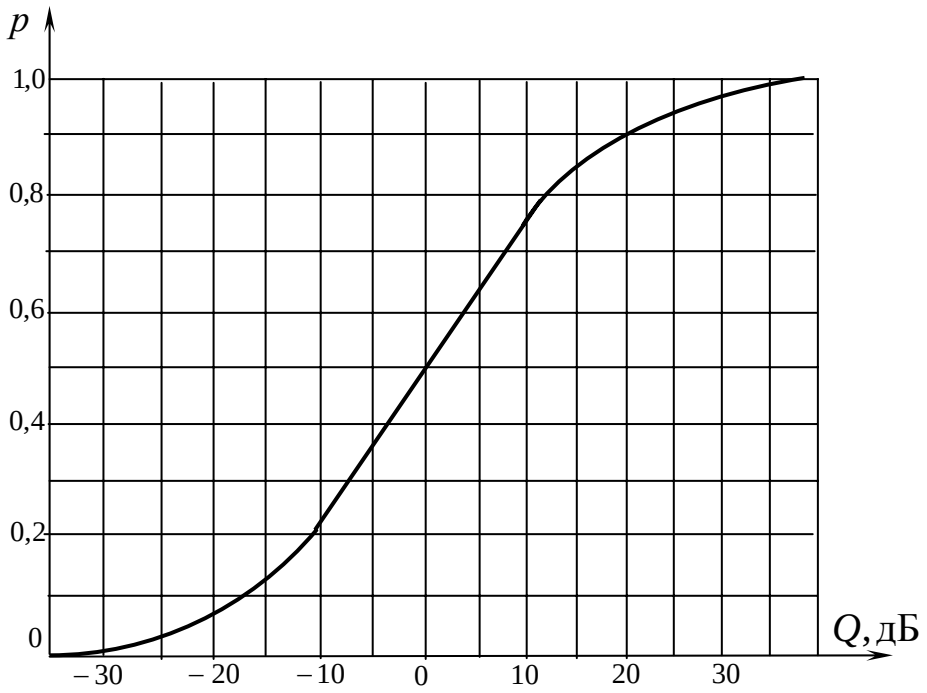


Рис. 7.5. Зависимость коэффициента восприятия формант p от относительного уровня интенсивности формант Q

С учетом ранее определенных значений рассчитываются спектральный индекс артикуляции речи в i-й спектральной полосе частотного диапазона

$$R_i = p_i k_i \tag{7.5}$$

и интегральный индекс артикуляции речи

$$R = \sum_i R_i . \tag{7.6}$$

Словесная разборчивость речи определяется как

$$W = \begin{cases} 1{,}54R^{0{,}25}\left[1-\exp(-11R)\right], & \text{если } R < 0{,}15; \\ 1-\exp\left(-\dfrac{11R}{1+0{,}7R}\right), & \text{если } R \geq 0{,}15. \end{cases} \tag{7.7}$$

Рассмотрим некоторые особенности акустических и виброакустических исследований ВП.

На рис. 7.6 схематично показано выделенное помещение с некоторыми важными потенциальными каналами утечки акустической и виброакустической информации, к которым относятся оконные и дверные проемы, стены и перегородки, перекрытия потолка и пола, система вентиляции, система отопления.

Согласно схеме помещения акустические исследования необходимо проводить для ограждающих конструкций (дверные проемы, стены и перегородки, перекрытия потолка и пола), а виброакустические – для инженерных конструкций (системы отопления и вентиляции), окон и железобетонных элементов ограждающих конструкций.

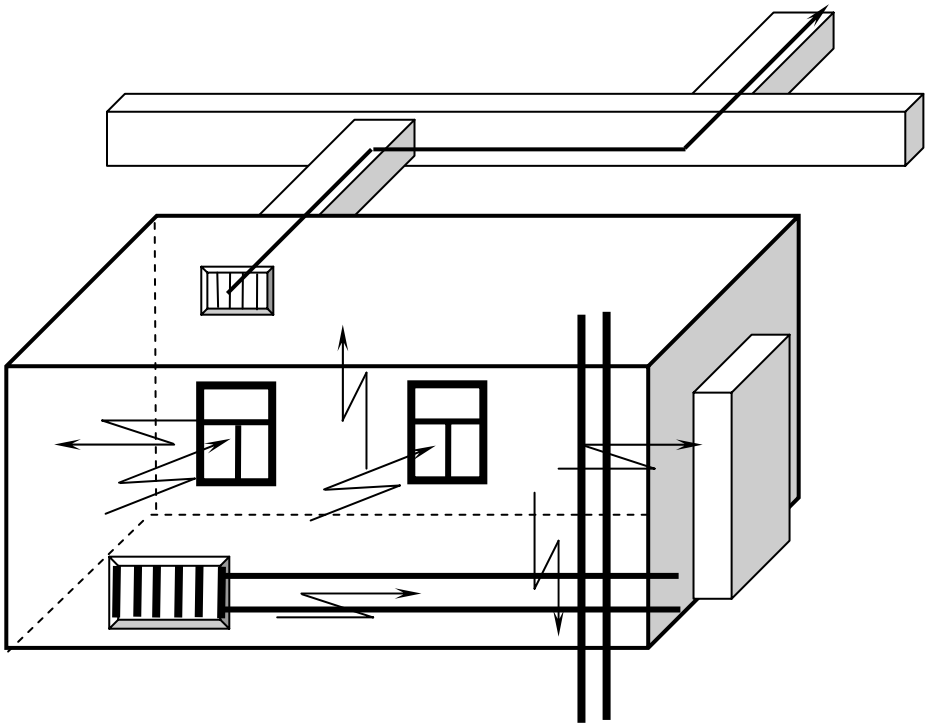


Рис. 7.6. Схема выделенного помещения

При акустических измерениях измерительные приборы располагаются согласно стандартной схемы – излучатель тестового сигнала (экранированная акустическая колонка) располагается на расстоянии 1,0 м от конструкции на высоте 1,5 м от пола; первый микрофон, измеряющий уровень падающей на конструкцию звуковой волны, располагается на расстоянии 0,5 м перед конструкцией; второй микрофон, измеряющий уровень прошедшей через конструкцию звуковой волны, устанавливается на расстоянии 0,5 м за конструкцией (рис. 7.7).

Если стена однородна, то достаточно одного или двух замеров вдоль стены. Если же стена неоднородна или имеет трещины и отверстия, то число контрольных точек необходимо увеличить, располагая их через 1,5…2 м друг от друга [38]. Для неоднородной стены измерению подлежит каждый ее элемент в отдельности и выводы делаются по наиболее «слабому» элементу.

Аналогично выполняются измерения и по виброакустическому каналу как при первоначальных исследованиях, так и при проверке эффективности средств активной звуковой защиты.

Измеритель вибрационных ускорений (акселерометр) крепится плотно к стене с противоположной стороны с помощью специального клея или приспособлений. Крепление акселерометра к рыхлой штукатурке, обоям и прочим мягким покрытиям недопустимо, так как в этом случае результаты измерений будут ошибочны из-за гашения виброколебаний этими материалами.

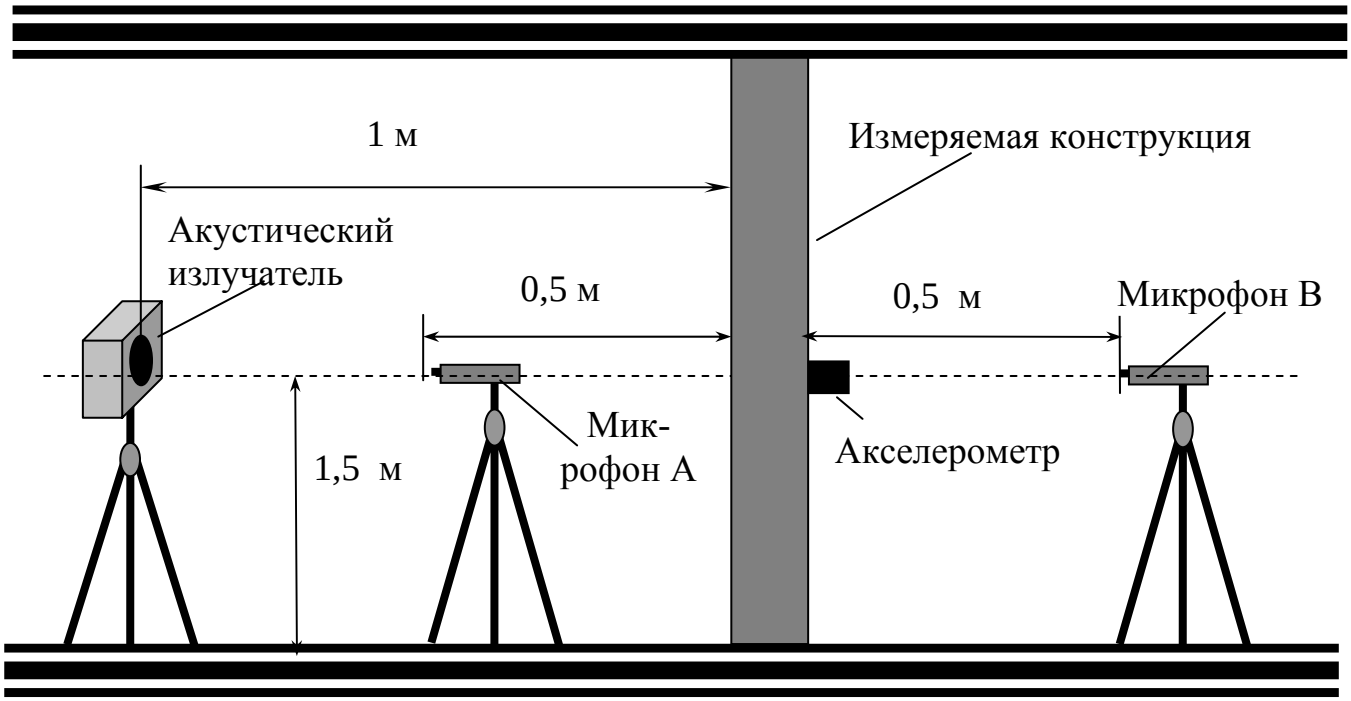


Рис. 7.7. Схема измерения акустических и виброакустических характеристик стены (перегородки)

На рис. 7.8 показана типовая схема измерения перекрытия пола. Расположение акустического излучателя согласно регламентирующим документам может быть иным, чем показано на схеме – допускается его установка на месте источника звука (рабочий стол руководителя, трибуна для выступлений и т.д.). При этом размещение датчиков не меняется.

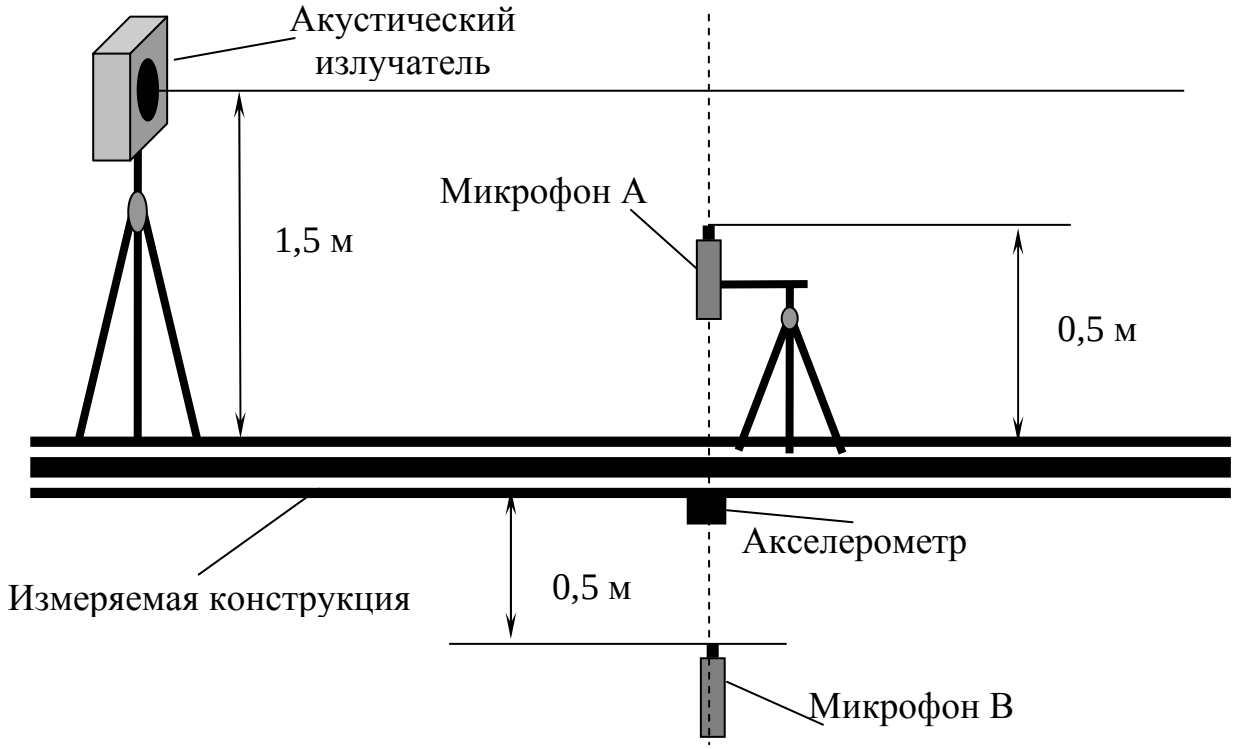


Рис. 7.8. Схема измерения акустических и виброакустических характеристик перекрытия пола

Схема измерения перекрытия потолка несколько отличается от схемы измерения перекрытий пола. Излучатель в обоих случаях размещается над полом, а микрофоны А и В по обе стороны ограждающей конструкции. При измерениях перекрытия потолка микрофон А размещается под потолком на расстоянии 0,5 м и развернут вертикально вниз (к источнику тест-сигнала). Микрофон В располагается над полом вышерасположенного помещения (т.е. над перекрытием потолка) на высоте 0,5 м и направлен вертикально вниз. Расположение микрофона В не зависит от наличия фальш-потолка.

Вибрационный канал утечки надо рассматривать (кроме окон) на границе контролируемой зоны, так как внутри зоны перехват информации обязаны исключить службы защиты информации заказчика.

На рис. 7.9 показана схема измерения акустических характеристик двойного дверного проема.

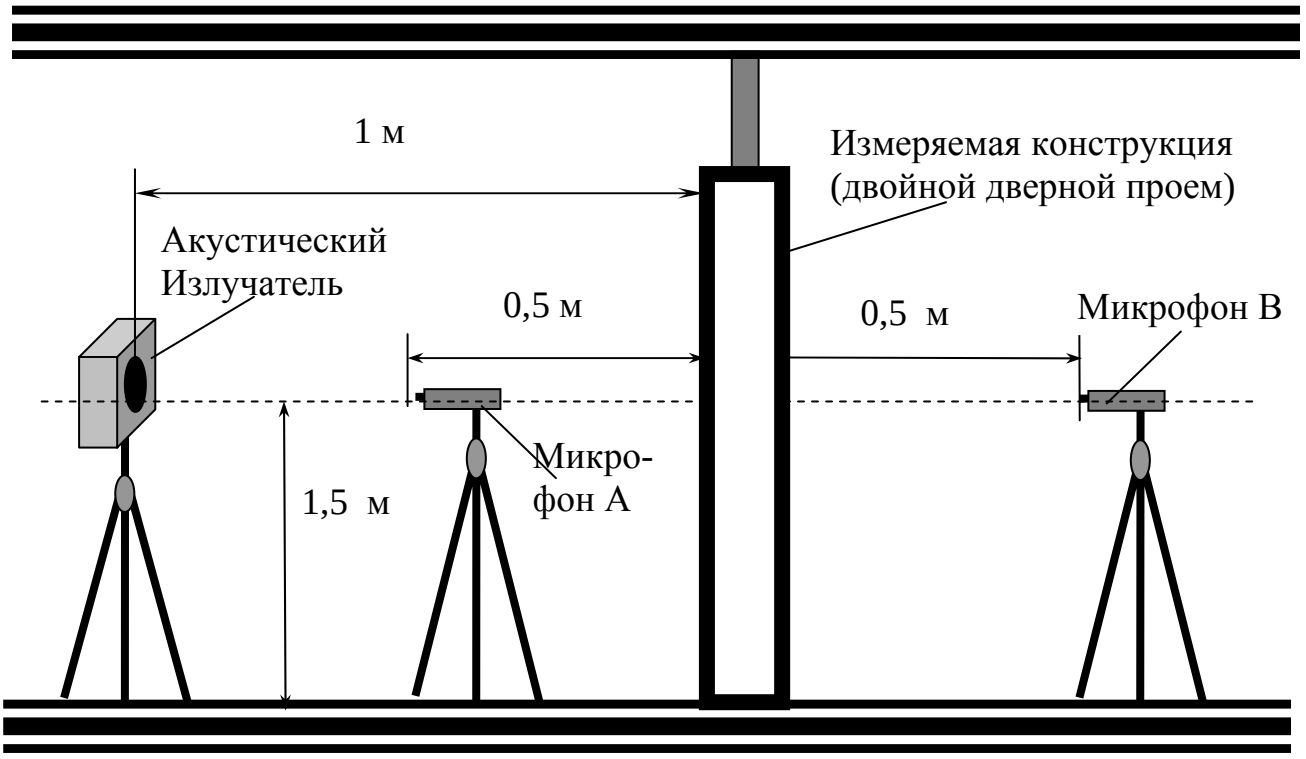


Рис. 7.9. Схема измерения акустических характеристик двойного дверного проема

При акустических измерениях необходимо следить, чтобы полотна дверей были плотно прикрыты и имели звукопоглощающие уплотнения.

На рис. 7.10 показана схема измерений на окне. Следует заметить, что окна в общем случае могут служить оптическим, акустическим, виброакустическим и оптико-электронным каналами утечки речевой информации. Если окна расположены на нижних этажах, то проведение акустических измерений на звукоизоляцию оконных проемов не представляет особого труда. Они проводятся по рассмотренной схеме.

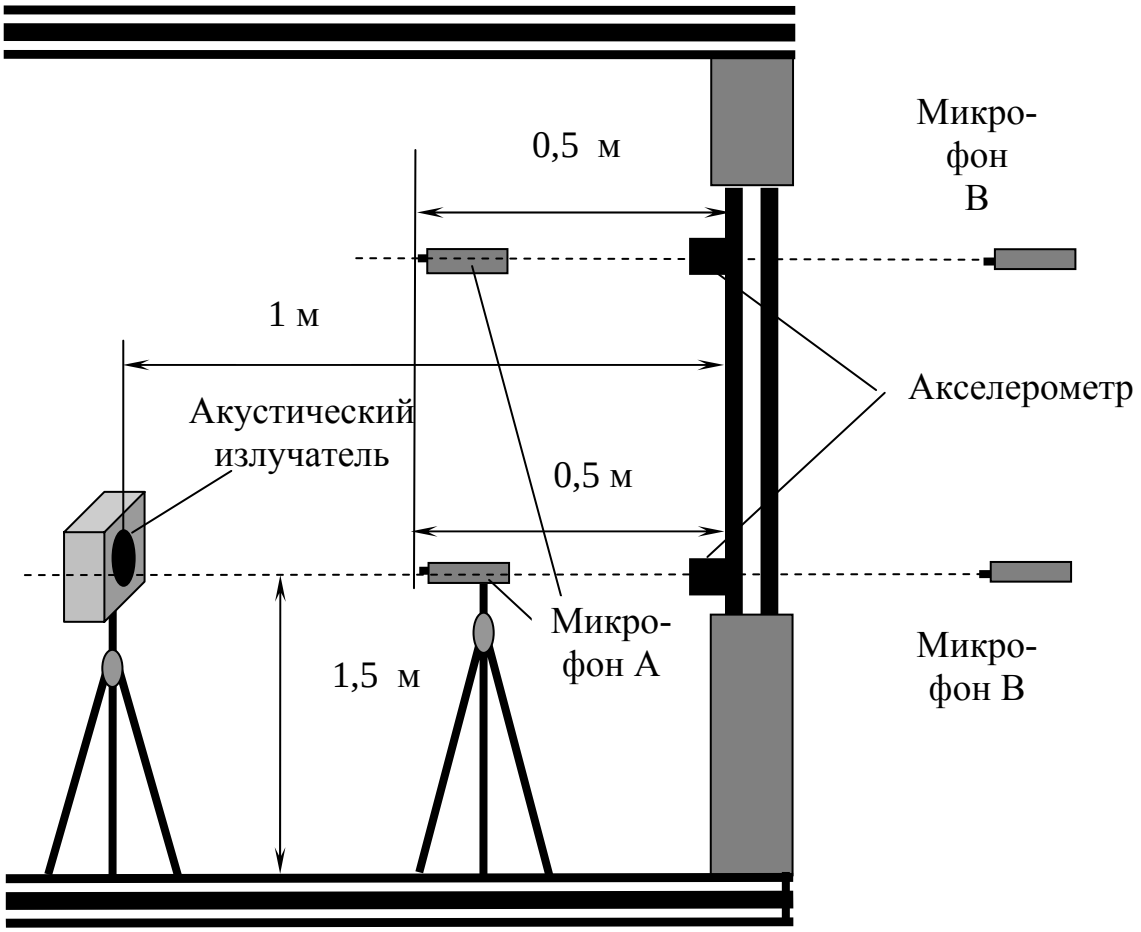


Рис. 7.10. Схема измерений на окне

Измерения защищенности по вибрационному каналу на остеклении окон с помощью оптико-электронной аппаратуры дистанционного прослушивания речи надо проводить с учетом некоторых особенностей, связанных с вертикальными размерами окон. Верхняя часть окон в большинстве случаев расположена значительно выше осевой линии акустического излучателя (выше 1,5 м от пола).

При проведении измерений в нижней и верхней частях окна на одинаковых предписанных расстояниях микрофона А (0,5 м) от плоскости стекол значение уровня падающей звуковой волны в верхней части окна будет на 3…8 дБ ниже, чем в нижней части [38].

При расчетных соотношениях сигнал/шум вблизи нормативных значений это может привести к ошибочным выводам. Поэтому для исключения подобной ситуации необходимо повторить измерения, поместив микрофон напротив центров верхних фрамуг.

Измерение в каналах вентиляционной системы производится по схеме, представленной на рис. 7.11. Излучатель располагается вблизи входа канала вентиляции на высоте 1,5 м от пола (расстояние от стены в 1 м не регламентируется). Микрофон А устанавливается на расстоянии в 0,5 м по нормали к плоскости вентиляционной решетки с ориентацией на нее.

Микрофон В устанавливается в плоскости ближайшего по ходу вентиляционного канала окна также с ориентацией на решетку окна. Это связано с тем, что при непреднамеренном прослушиванием, например, во время ремонтно-профилактических работ, ухо постороннего может оказаться в этой же плоскости.

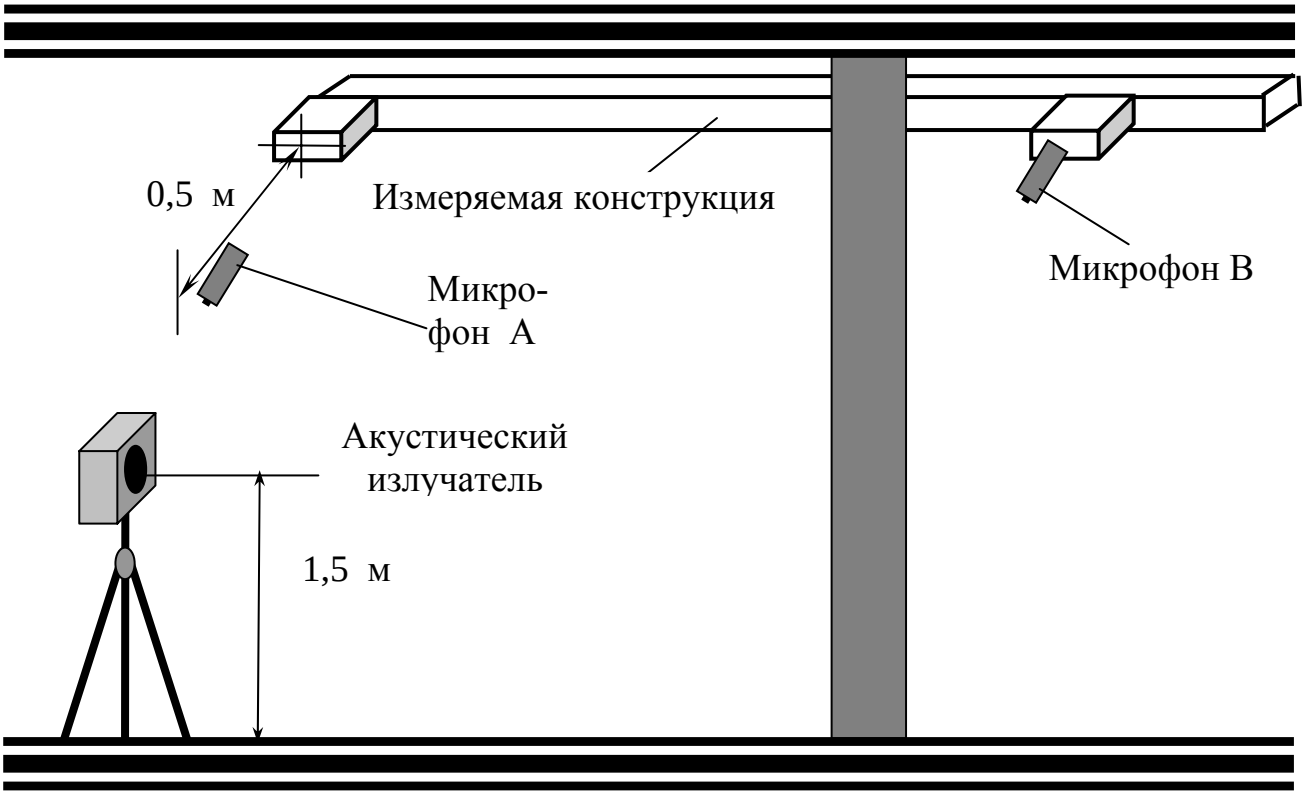


Рис. 7.11. Схема измерения в канале системы вентиляции

В коробе распространяется сферическая звуковая волна со снижением звукового давления пропорционально третьей степени расстояния от источника звука. Поэтому расчеты защищенности в плоскости решетки и на расстоянии 0,5 м будут отличаться в несколько раз [38]. Уровень тестирующего сигнала зависит от характера решаемой задачи, общей рекомендацией является установка его не менее 10 дБ выше уровня шумов [38].

При измерениях на окнах при одиночных стеклах вполне достаточно давления 60…65 дБ, для стеклопакетов – 70…80 дБ. При измерениях на дверных проемах общего типа, в том числе и двойных, необходим уровень тестирующего сигнала 70…75 дБ, а для дверей с усиленной звукоизоляцией – до 90 дБ. Для стен и капитальных перегородок уровень тест-сигнала необходимо поднимать до допустимого максимума.

Измерения на системе отопления (рис. 7.12), представляющей собой виброакустический канал утечки речевой информации, на трубах отопления рекомендуется проводить в следующем порядке [38].

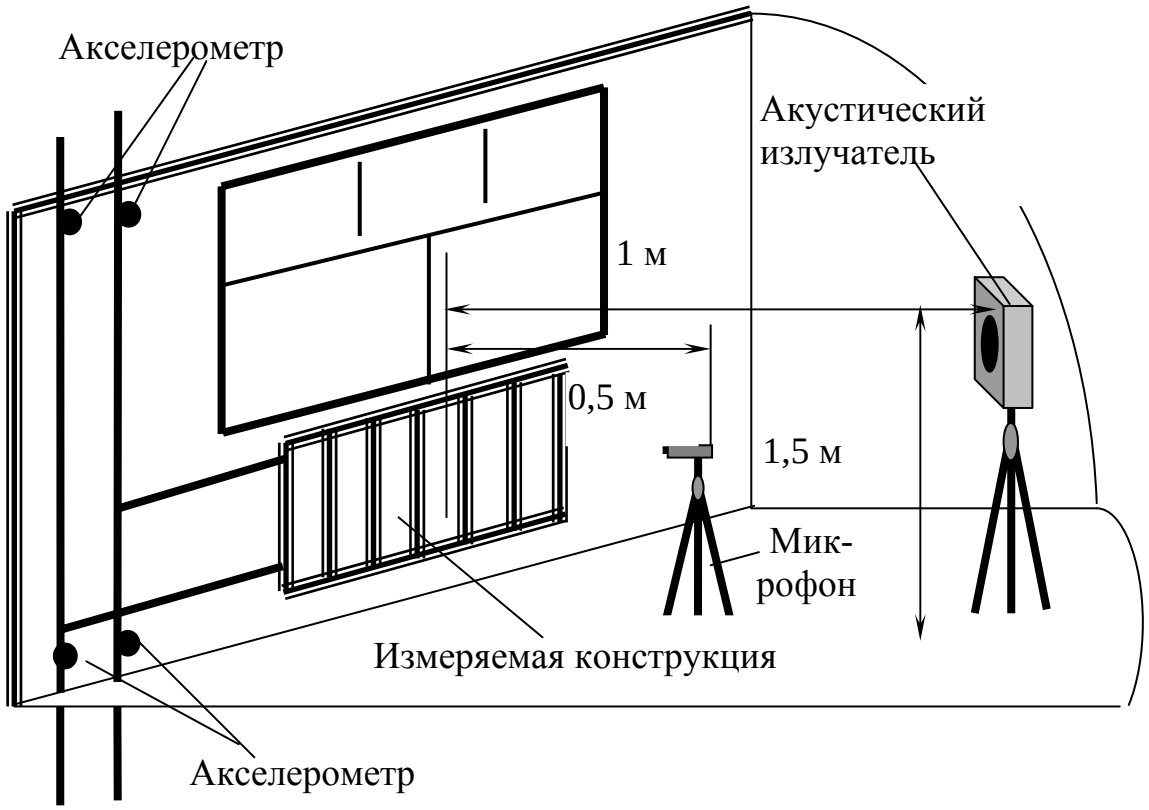


Рис. 7.12. Схема измерений на системе отопления

Акустический излучатель располагается относительно плоскости батареи, являющейся наиболее эффективным приемником звуковой волны. Микрофон А направляется на излучатель и располагается на расстоянии 0,5 м от плоскости батареи по ее центру.

Если границей контролируемой зоны являются ограждающие конструкции выделенного помещения, то акселерометр закрепляется поочередно на трубах на расстоянии 10…15 см от места выхода трубы из выделенного помещения.

Если же границей контролируемой зоны являются стены здания, в котором находится контролируемое помещение, то в связи со значительным затуханием вибрационного тест-сигнала до точки установки акселерометра прямой замер защищенности становится невозможным. В подобном случае надо размещать акселерометр на таком расстоянии от выделенного помещения, на котором тест-сигнал надежно измеряется, а результаты измерения защищенности от утечки удовлетворяют требованиям. На этом основании делается вывод, что на границе контролируемой зоны вследствие дальнейшего затухания тест-сигнала результаты будут еще лучше.

Другой метод заключается в измерении реального затухания в канале утечки. Суть его заключается в генерации в канал с большим затуханием достаточно мощного вибрационного тест-сигнала не от акустической колонки, а непосредственно от вибропреобразователя (ВП), позволяющего

создавать тест-сигнал с уровнем 120…130 дБ относительно 10^{-6} м/с^2 (рис. 7.13). Заметим, что акустическая колонка с уровнем звукового давления 100 дБ не способна создать в трубе вибрационный сигнал более 75…80 дБ [38].

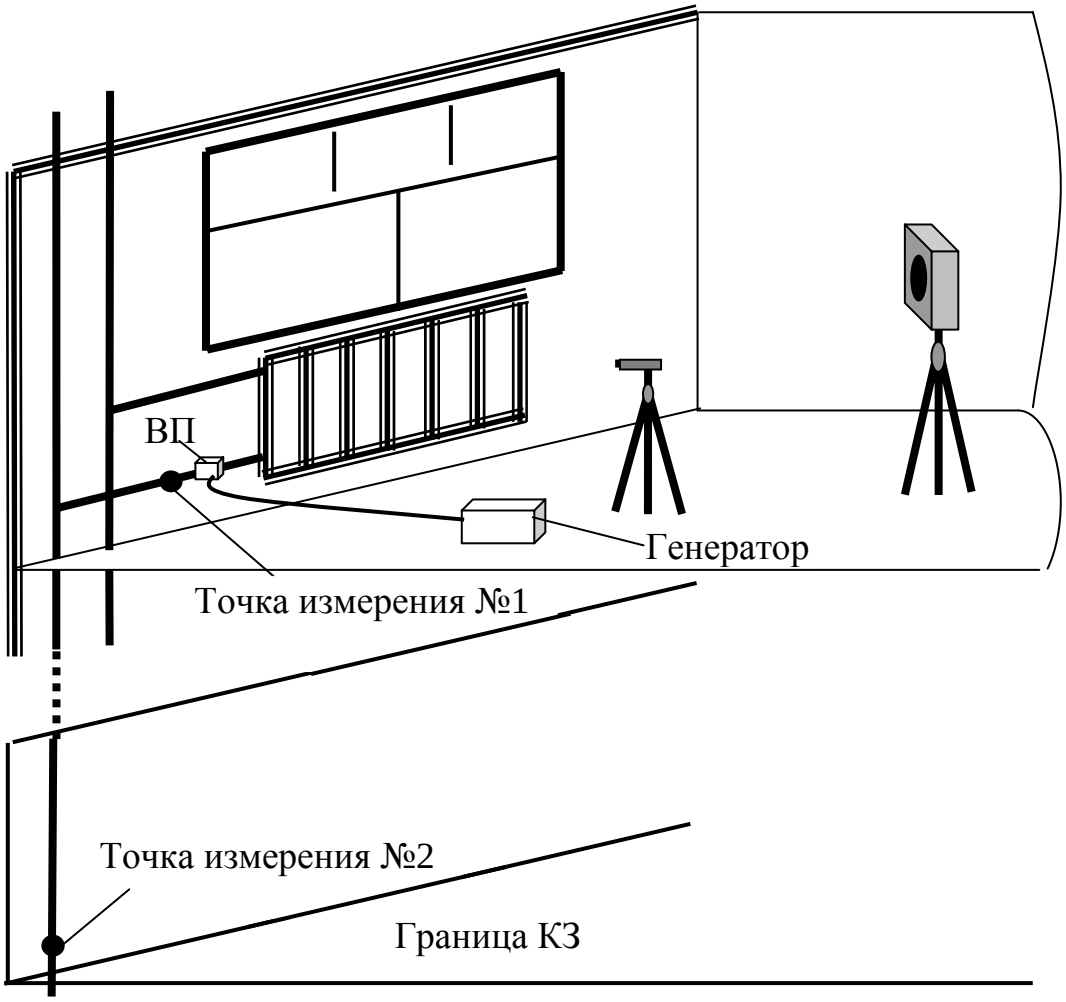


Рис. 7.13. Схема измерения в вибрационном канале с учетом реального затухания

Для определения затухания необходимо измерить уровень тест-сигнала во всех пяти октавных полосах в 10…15 см от возбуждающего вибропреобразователя (точка № 1), а второй замер сделать на границе контролируемой зоны (точка № 2). Разность между значениями этих двух измеренных уровней вибросигнала и будет являться реальным затуханием в канале.

Обычно тест-сигнал удается выделить над уровнем шумов на расстоянии не менее 50…100 м от источника вибросигнала. Если тест-сигнал не выявляется на границе контролируемой зоны, то допустимо точку ввода тест-сигнала перенести к границе контролируемой зоны на расстояние, при котором тест-сигнал надежно выявляется, и измерить реальное затухание на этом участке.

Если реальное затухание удается измерить не во всех октавных полосах, то рекомендуется для тех октав, в которых затухание определить не удалось [38], принять минимальное значение из полученных затуханий по октавным полосам. В большинстве случаев значение уровня тест-сигнала в точке № 2 соизмеримо с уровнем шумов и фактически измеряется смесь сигнала с шумом. Поэтому в этой точке необходимо измерять раздельно уровни шума (при выключенном вибропреобразователе) и смесь сигнала с шумом (при включенном вибропреобразователе).

Реальное затухание в каждой октавной полосе рассчитывается по формуле:

$$\Delta V_i = V_{1i} - 20\lg\sqrt{10^{\frac{V_{2i,\text{с+ш}}}{10}} - 10^{\frac{V_{2i,\text{ш}}}{10}}}, \qquad (7.8)$$

где для каждой *i*-й октавной полосы: ΔV_i – реальное затухание, дБ; V_{1i} – уровень тест-сигнала в точке его ввода (точка № 1), дБ; $V_{2i,\text{с+ш}}$ – уровень тест-сигнала в смеси с шумом на границе контролируемой зоны (точка № 2), дБ; $V_{2i,\text{ш}}$ – уровень шума на границе контролируемой зоны (точка № 2), дБ.

В случае невыполнения норм защищенности по акустическим и виброакустическим каналам утечки при исчерпанных возможностях средств пассивной защиты применяются средства активной защиты (САЗ), принцип работы которых заключается в зашумлении каналов утечки речевой информации.

Основной недостаток САЗ состоит в создании для работающих в выделенном помещении дискомфорта, связанного с появлением дополнительных шумов на частотах звукового диапазона. Больше неудобств доставляет не акустическое зашумление с помощью колонок, а защищенные вибропреобразователями стекла окон. Стекла являются конструкцией мембранного типа и при возбуждении вибропреобразователями обладают хорошей звукоизлучающей способностью (особенно стекла больших размеров). В связи с этим оптимальное расположение вибродатчиков на стеклах и квалифицированная настройка амплитудно-частотных характеристик (АЧХ) генератора шумовых сигналов являются важнейшей задачей для специалистов. В среднем рекомендуется на $1\,\text{м}^2$ стекла размещать 2 вибродатчика. При большом числе фрамуг с различными свойствами необходимо с целью оптимизации применять генераторы типа «Шорох» с тремя независимо настраиваемыми по АЧХ каналами.

Сложным является и вопрос определения местоположения контрольных точек на плоскости стекла для проведения измерений и оценки эффективности САЗ с учетом недопустимости оценки по одной точке. Приблизительная схема размещения контрольных точек рекомендуется в [38].

Нет указаний в руководящих документах, какая из поверхностей многослойного остекления является самой опасной с точки зрения съема информации лазерными устройствами. Теоретически каждая из поверхностей способна отражать лазерный луч и поэтому опасна. Наиболее сложным для защиты является вариант, когда датчики зашумления располагаются на внутренней поверхности внутреннего стекла, а оценка защищенности проводится на самой наружной поверхности.

Зашумление ограждающих конструкций их твердых материалов производится установкой вибропреобразователей на каждый элемент конструкции.

Трубы водоснабжения, отопления, канализации зашумляются достаточно просто. Если имеется система жестко связанных труб, то допускается установка одного вибропреобразователя, размещенного примерно посередине этой системы, а контрольные точки выбираются вблизи выхода труб из выделенного помещения.

Дверные проемы обычно зашумляются установкой акустической колонки в тамбуре двойной двери, но значительно эффективнее осуществлять защиту установкой колонки у косяка наружной двери. В этом случае зашумляется опасный сигнал уже частично поглощенный двумя дверьми и требуемый уровень зашумляющего сигнала может быть установлен значительно ниже. В обратном направлении шумовой сигнал ослабляется также двумя дверьми, что приводит к нормальным условиям работы в выделенном помещении.

При защите систем вентиляции наиболее эффективна установка зашумляющей акустической колонки в канале на расстоянии не менее 1,5 м от плоскости его выхода в помещение. Этим обеспечивается необходимое зашумление при невысоких уровнях громкости колонки и отсутствии значительного шума в помещении.

7.2.3.2. Специальные исследования акустоэлектрических преобразований

Под акустоэлектрическим преобразованием понимают преобразование механической энергии акустического сигнала отдельными устройствами в электрический сигнал (напряжение, ток, заряд), модулированный по закону изменения акустического сигнала. В свою очередь, электрические сигналы создают электрическое и магнитное поля, которые также могут образовать канал утечки информации. Опасность акустоэлектрического канала утечки состоит в том, что наведенные электрические сигналы несмотря на свой низкий уровень могут распространяться по проводным линиям за пределы контролируемой зоны и перехватываться средствами технической разведки.

В большинстве случаев акустоэлектрическое преобразование имеет обратимый характер, и тогда имеют дело с электроакустическим преобразованием, которое с точки зрения утечки информации не представляет интереса.

Акустоэлектрическим эффектом обладают многие элементы электронных технических средств обработки информации и вспомогательных технических средств. Прежде всего, это моточные изделия (трансформаторы, дроссели, реле и т.п.), в которых в соответствии с законом электромагнитной индукции, открытым Фарадеем, наводится ЭДС при движении проводников в магнитном поле под действием энергии звуковой волны. Магнитное поле всегда присутствует в ферромагнитных сердечниках за счет остаточной индукции.

Акустоэлектрическими преобразователями являются также конденсаторы, у которых обкладки под действием звука могут перемещаться друг относительно друга в поперечном направлении, изменяя емкость конденсатора.

Достаточно часто причиной акустоэлектрических преобразований являются керамические конденсаторы, содержащие материалы с пьезострикционным эффектом и являющиеся подобием пьезоэлектрического микрофона.

Микрофонный эффект в перечисленных случаях не всегда ярко выражен, сигнал акустоэлектрического преобразования может быть меньше допустимой нормы, но это каждый раз необходимо доказывать исследованиями.

Кроме каналов прямого акустоэлектрического преобразования существуют и модуляционные высокочастотные каналы акустоэлектрических преобразований, суть которых сводится к модуляции сигналов высокочастотных генераторов по амплитуде или частоте речевым сигналом за счет воздействия последнего на конденсаторы или катушки индуктивности в задающих контурах. Модулированный высокочастотный сигнал генератора при относительно большой мощности может создавать информативные побочные электромагнитные излучения и распространяться по проводным линиям.

Для прямого акустоэлектрического преобразования измерение величины сигналов речевого диапазона частот исследуемого технического средства (ТС) рекомендуется типовая схема (рис. 7.14) [38]. В конкретных реальных условиях можно применять не только указанные приборы, но и другие сертифицированные их аналоги с не уступающими характеристиками.

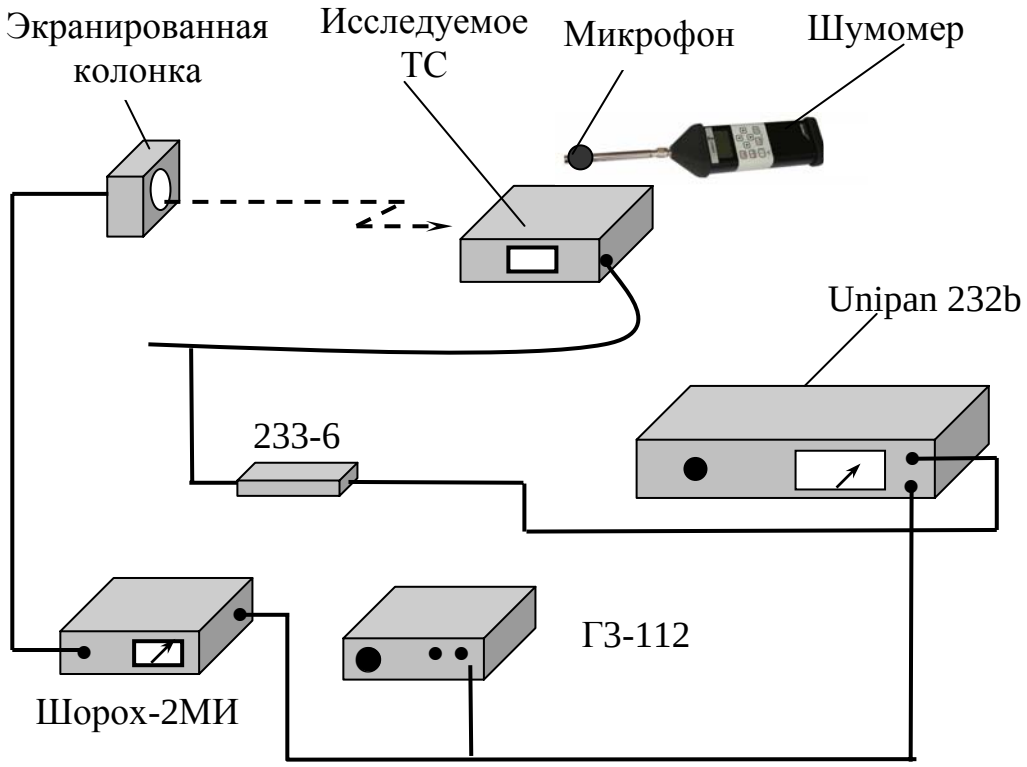


Рис. 7.14. Типовая схема измерения прямого акустоэлектрического преобразования

Исследуемое техническое средство может быть подключено к реальной отходящей линии, к имитатору или находиться в режиме холостого хода. К отходящей линии подключается измерительный нановольтметр непосредственно или бесконтактно через токовый трансформатор. Подключение измерительного нановольтметра необходимо выполнять по всем возможным вариантам: симметрично, несимметрично, по разбитым парам, по нескольким проводам (в случае применения токового трансформатора) и т.д.

Для усиления слабого сигнала акустоэлектрического преобразования прямое подключение измерительного прибора производится через предусилитель типа 233-6 для Unipan 232b. Токовый трансформатор может охватывать один или несколько проводов. Следует помнить, что токовый трансформатор измеряет ток в линии или алгебраическую сумму токов, а нормируется напряжение. Напряжение определяется умножением тока на эквивалентное сопротивление линии или внутреннего сопротивления источника сигнала.

Экранированную акустическую колонку, создающую тестирующий звуковой сигнал с характеристиками, задаваемыми генератором Шорох-2МИ, обычно размещают на расстоянии 1 *м* от исследуемого технического средства. Такое расстояние выбирается из соображений обеспечения требуемого уровня звукового давления и допустимого уровня электромагнит-

ных наводок от колонки на техническое средство. Электромагнитные наводки тест-сигнала при неудачно выбранном удалении колонки от технического средства, неправильной схеме заземления измерительного комплекса и отсутствии экранирования симметричных кабелей могут превышать по величине сигнал акустоэлектрического преобразования (АЭП).

Чтобы убедиться в том, что измеряется именно сигнал АЭП, необходимо снизить уровень тест-сигнала, прикрыв лицевую панель колонки звукопоглощающей шторкой (ни в коем случае нельзя снижать уровень тест-сигнала регулировкой генератора, так как в этом случае снизится уровень электромагнитной наводки). В результате таких действий при отсутствии электромагнитной наводки от колонки показания измерительного нановольтметра не должны измениться. В противном случае необходимо варьировать взаимным расположением генераторной и измерительной части комплекса до получения положительного результата.

Уровень тестирующего звукового сигнала непосредственно у технического средства измеряется шумомером.

Рекомендуется следующий порядок проведения измерений. После включения, прогрева и калибровки всех средств измерения оператор плавно изменяет частоту звукового генератора в заданном диапазоне частот при звуковом давлении 74…94 дБ. Как правило, огибающая сигнала АЭП характеризуется пиками и провалами. Рекомендуется фиксировать наибольшие пики. При использовании нановольтметра Unipan 232b надо следить за подстройкой фазы опорного сигнала на «подозрительных» частотах.

Задавать перестройку частоты шагами более 10 Гц недопустимо во избежание пропуска узкополосных сигналов АЭП.

Исследуемое техническое средство необходимо проверять во всех возможных режимах его работы и принимать за результат наибольшее значение опасного сигнала.

Опасными являются каналы утечки информации, образованные встроенными в ТС автогенераторами и усилителями с обратной связью, способными модулировать колебания под воздействием звуковых сигналов. Высокочастотные сигналы автогенераторов (несущая частота) могут быть модулированы по различным видам модуляции, чаще всего по амплитудной или частотной.

Паразитная генерация усилителей возникает из-за неконтролируемой положительной обратной связи за счет конструктивных особенностей схемы или за счет старения элементов. Самовозбуждение может возникнуть и при отрицательной обратной связи из-за того, что на частотах, где усилитель вместе с цепью обратной связи вносит сдвиг фазы на 180°, отрицательная обратная связь превращается в положительную. Усилитель может находиться на границе устойчивости и при малейших изменениях коэффи-

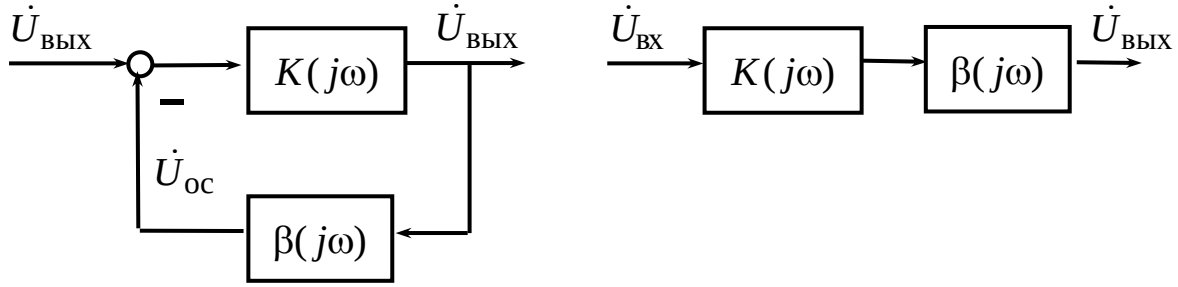
циента передачи перейти в неустойчивый режим с паразитной высокочастотной генерацией.

Самовозбуждение усилителей обычно происходит на высоких частотах, выходящих за пределы рабочей полосы частот (вплоть до КВ и УКВ диапазонов).

Частота самовозбуждения модулируется акустическим сигналом, поступающим на усилитель, и излучается в эфир как обычным радиопередатчиком. Дальность распространения такого сигнала определяется мощностью усилителя и особенностями диапазона радиоволн.

Независимо от схемотехнических особенностей усилителей с отрицательной обратной связью их структурная схема может быть приведена к виду, показанному на рис. 7.15, *а*.

На структурной схеме обозначены: $K(j\omega)$ – комплексный коэффициент передачи собственно усилителя, $\beta(j\omega)$ – комплексный коэффициент передачи звена отрицательной обратной связи. В простейшем случае β может являться безынерционным звеном и показывать какая часть выходного напряжения $\dot{U}_{\text{вых}}$ поступает на вход усилителя в качестве сигнала обратной связи $\dot{U}_{\text{ос}}$.



а *б*

Рис. 7.15. Замкнутая (*а*) и разомкнутая (*б*) структурные схемы усилителя

Согласно теории автоматического управления амплитудно-фазовая характеристика (АФХ) замкнутой схемы с отрицательной обратной связью определяется выражением $K_{\text{замк}}(j\omega)=\dfrac{K(j\omega)}{1+K(j\omega)\beta(j\omega)}$, а АФХ разомкнутой структурной схемы в согласно рис. 7.15, *б* соответствует выражение $K_{\text{р}}(j\omega)=K(j\omega)\cdot\beta(j\omega)$.

АФХ разомкнутой структурной схемы усилителя при наличии более двух инерционных звеньев, необходимая для определения устойчивости усилителя в замкнутом состоянии по критерию Найквиста (кривая 1), показана на комплексной плоскости рис. 7.16.

Напомним, что согласно критерию Найквиста работа усилителя в замкнутом состоянии будет устойчива, если его АФХ в разомкнутом состоянии не охватывает критическую точку с координатами (–1; $j0$), а структурная схема разомкнутой системы состоит из устойчивых звеньев. Второе условие в усилителях обычно всегда выполняется.

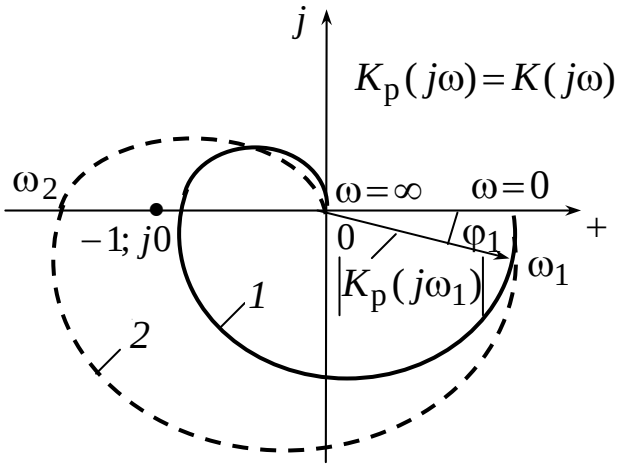


Рис. 7.16. Амплитудно-фазовые характеристики разомкнутой структурной схемы усилителя

На рис. 7.16 для некоторой частоты ω_1 на кривой 1, соответствующей устойчивой работе усилителя, показано положение изображающего вектора $K_{\text{р}}(j\omega_1)$ (его модуль и аргумент φ_1, являющийся фазовым сдвигом между входным и выходным напряжениями).

При увеличении коэффициента передачи разомкнутой схемы $|K_{\text{р}}(j\omega)|$, что возможно за счет увеличения K и β, АФХ разомкнутой структурной схемы может охватить критическую точку (пунктирная кривая 2 на рис. 7.16) и усилитель перейдет в неустойчивый (колебательный) режим работы. На некоторой частоте ω_2 фазовый сдвиг станет равным 180°, а входное и выходное напряжения окажутся в фазе, т.е. отрицательная обратная связь станет положительной. Равенство фазового сдвига ста восьмидесяти градусам при достаточных запасах устойчивости по модулю и по фазе не приводит к самовозбуждению усилителей.

Усилители должны исследоваться при изменении напряжения питания в допустимых пределах и при перегрузках по входу и выходу.

Для измерений сигнала модуляционного акустоэлектрического преобразования в высокочастотной области применяются другие измерительные приборы и схема выглядит несколько иначе (рис. 7.17).

Основным элементом измерительного комплекса является измерительный приемник (анализатор спектра), имеющий выходы по промежуточной частоте (ПЧ) и по низкой частоте (НЧ). На вход приемника могут подключаться либо антенна (если проводятся измерения ПЭМИ), либо пробник (если проводятся измерения в отходящей линии). К выходу ПЧ измерительного приемника могут подключаться измеритель модуляции или низкочастотные анализаторы спектра. В первом случае проводится непосредственное измерение, а во втором – измерение методом боковых частот.

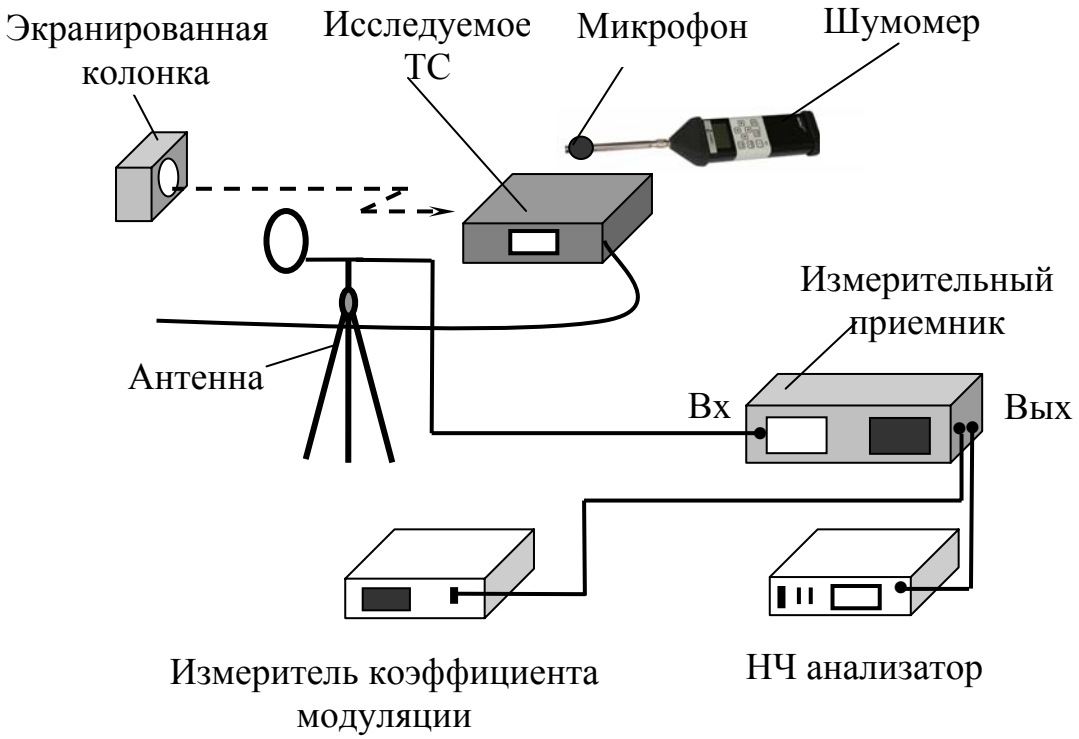


Рис. 7.17. Схема измерения сигнала модуляционного АЭП

Для выявления факта модуляции на слух к низкочастотному выходу приемника подключаются головные телефоны. Подготовка к проведению измерений сводится к тщательному изучению исследуемого технического средства с целью выявления мест и режимов с наиболее вероятным появлением сигналов АЭП. Далее оператор измеряет все выявленные излучаемые или присутствующие в отходящих линиях сигналы автогенераторов, работающих в составе технических средств. Кроме этого, необходимо обязательно проводить дополнительный поиск сигналов в диапазоне частот от 10 кГц до 1000 МГц [38]. Все выявленные сигналы в этом диапазоне частот должны также проверяться на наличие модуляции.

7.2.3.3. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок

Побочные электромагнитные излучения и наводки (ПЭМИН) можно разделить на [39]:

- не предусмотренные в работе технических средств акустоэлектрические преобразования;
- паразитные связи и наводки;
- побочные низкочастотные излучения;
- побочные высокочастотные излучения.

Под низкочастотными излучениями понимают электромагнитные излучения с частотами слышимого звукового диапазона. Источниками таких излучений являются устройства и цепи, содержащие случайные и не случайные акустоэлектрические преобразователи с соединительными линиями.

К высокочастотным опасным излучениям относятся электромагнитные излучения от высокочастотных цепей, по которым циркулирует секретная или конфиденциальная информация. Источником таких излучений могут являться:

- усилители и логические элементы в режиме паразитной генерации;
- генераторы подмагничивания и стирания магнитофонов;
- гетеродины радио– и телевизионных приемников;
- элементы ВЧ-навязывания;
- устройства и узлы компьютерной техники.

Сигналы можно представлять функциями времени или в виде частотных спектров. При исследовании ПЭМИН сигналы обычно представляются в виде частотных спектров.

Если сигнал определяется гармонической функцией $A\cos(\omega t+\psi)$, то на шкале частот она определяется заданной амплитудой A и начальной фазой ψ ((рис. 7.18, *а*).

При комплексной форме записи косинусоиды

$$A\cos(\omega t+\psi)=\frac{A}{2}[e^{j(\omega t+\psi)}+e^{-j(\omega t+\psi)}] \qquad (7.9)$$

вводится чисто математическое понятие отрицательной угловой частоты, а шкала частот дополняется отрицательной полуосью. Амплитудный и фазовый спектр в этом случае изображаются парами ординат (рис. 7.18, *б*), соответствующих положительны и отрицательным значениям угловой частоты.

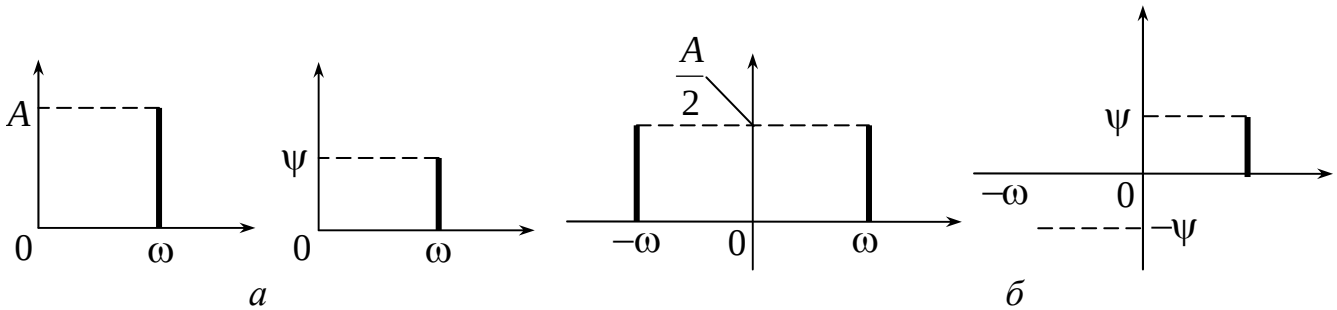


Рис. 7.18. Спектральное представление гармоники: *а* – обычное, *б* – для комплексной формы записи косинусоиды

Несинусоидальные сигналы могут быть разложены в ряд Фурье, т.е. представлены в виде дискретного ряда гармоник.

Напомним, что для тригонометрической формы записи ряда Фурье для функции

$$f(t)=\frac{a_0}{2}+\sum_{n=1}^{\infty}A_n\cos(n\omega_1 t-\psi_n) \qquad (7.10)$$

амплитуды A_n и начальные фазы ψ_n определяются формулами

$$A_n=\sqrt{a_n^2+b_n^2};\ \ \psi_n=\operatorname{arctg}\frac{b_n}{a_n}, \qquad (7.11)$$

где n – номер гармоники.

В (7.11) коэффициенты разложения

$$a_n=\frac{2}{T}\int_0^T f(t)\cos n\omega_1 t\,dt;\ \ b_n=\frac{2}{T}\int_0^T f(t)\sin n\omega_1 t\,dt, \qquad (7.12)$$

где T – период основной частоты, $\omega_1=2\pi/T$ – основная частота. Для комплексной формы записи ряда Фурье

$$f(t)=\frac{1}{2}\sum_{n=-\infty}^{\infty}\dot{A}_n e^{jn\omega_1 t} \qquad (7.13)$$

комплексные амплитуды определяются по формуле

$$\frac{1}{2}\dot{A}_n=\frac{1}{2}A_n e^{-j\psi_n}=\frac{1}{2}(a_n-jb_n)=\frac{1}{T}\int_0^T f(t)e^{-jn\omega_1 t}dt, \qquad (7.14)$$

в которой A_n,ψ_n,a_n,b_n вычисляются по ранее приведенным формулам.

Совокупность амплитуд соответствующих гармоник $\frac{1}{2}A_n=\frac{1}{2}A_{-n}$ (модулей комплексных коэффициентов ряда Фурье, отложенных против соответствующих положительных и отрицательных частот) представляет симметричный относительно оси ординат линейчатый амплитудный спектр.

Линейчатый фазовый спектр образуют аргументы (фазы) комплексных коэффициентов ряда Фурье.

Рассмотрим периодическую последовательность прямоугольных импульсов единичного уровня с периодом повторения, значительно превышающим длительность импульса (рис. 19, *а*), что характерно для средств цифровой обработки информации.

Характеристикой последовательности импульсов является скважность $N=T/t_1$.

Импульсу на оси ординат (рис. 7.19, *а*) соответствует временная функция

$$f(t)=\begin{cases}1 \ \text{при}\ -\dfrac{t_1}{2}<t<\dfrac{t_1}{2};\\ 0 \ \text{при}\ \dfrac{t_1}{2}<t<T-\dfrac{t_1}{2}.\end{cases}$$

Согласно (7.14) выражение для комплексных амплитуд определяется как

$$\dot{A}_n = \frac{2}{T}\int_{-\frac{t_1}{2}}^{\frac{t_1}{2}} e^{-jn\omega_1 t}dt = \frac{2t_1}{T}\frac{\sin\frac{n\omega_1 t_1}{2}}{\frac{n\omega_1 t_1}{2}} = \frac{2}{N}\cdot\frac{\sin\frac{n\pi}{N}}{\frac{n\pi}{N}}. \qquad (7.15)$$

На основании (7.15) можно построить спектр.

Если в последнем выражении обозначить $\frac{n\pi}{N} = x$, то очевидно, что огибающая спектра, показанная на рис. 7.19, *б*, описывается простым выражением $\dot{A}_n = \frac{2t_1}{T}\cdot\frac{\sin x}{x}$.

Число спектральных линий между началом отсчета по шкале частот (или номеров гармоник) и первым нулем огибающей равно числу спектральных линий между соседними нулями и составляет $N - 1$. Положение нулей огибающей спектра на оси частот не зависит от периода T, а определяется только длительностью импульса. При этом коэффициенты ряда заданного периодического сигнала обратно пропорциональны периоду (или скважности импульсов). С ростом T огибающая снижается, стремясь при $T \to \infty$ совпасть с осью абсцисс.

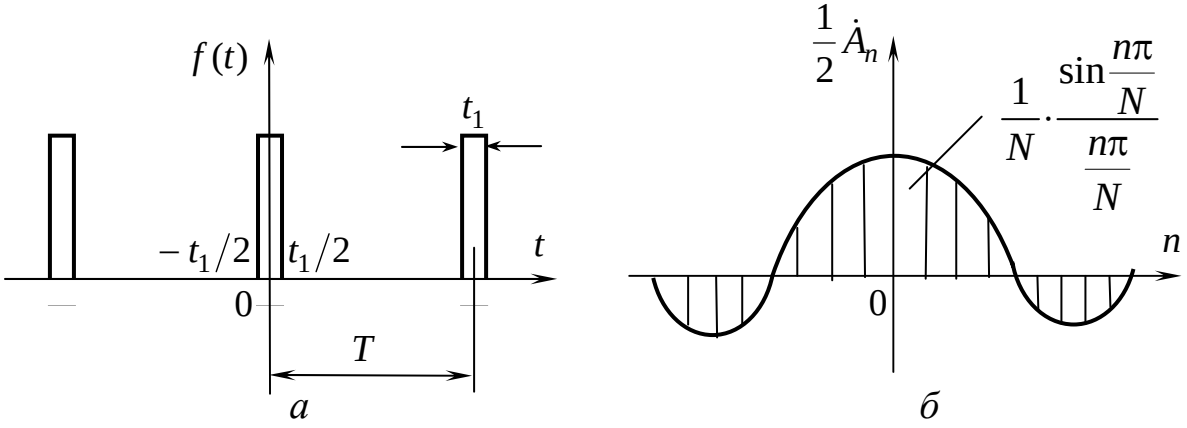


Рис. 7.19. Последовательность прямоугольных импульсов (*а*) и ее спектр (*б*)

Перепишем временную функцию $f(t) = \frac{1}{2}\sum_{n=-\infty}^{\infty}\dot{A}_n e^{jn\omega_1 t}$ в следующем виде:

$$f(t) = \frac{1}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\pi}{\omega_1}\dot{A}_n e^{jn\omega_1 t}[n\omega_1 - (n-1)\omega_1 = \frac{1}{2\pi}\sum_{n=-\infty}^{\infty}\frac{T}{2}\dot{A}_n e^{jn\omega_1 t}\Delta(n\omega_1). \quad (7.16)$$

Здесь $\Delta(n\omega_1)=n\omega_1-(n-1)\omega_1$ – частотный интервал между составляющими ряда Фурье. Так как $\dot{A}_n=\frac{2}{T}\int\limits_{-\frac{T}{2}}^{\frac{T}{2}} e^{-jn\omega_1 t}dt,$ то

$$f(t)=\frac{1}{2\pi}\sum_{n=-\infty}^{\infty} e^{jn\omega_1 t}\Delta(n\omega_1)\int\limits_{-\frac{T}{2}}^{\frac{T}{2}} f(t)e^{-jn\omega_1 t}dt. \qquad (7.17)$$

По мере возрастания периода T интервал $\Delta(n\omega_1)$ сокращается, а линейчатый спектр все более сгущается при уменьшении модулей A_n комплексных амплитуд. При $T\to\infty$ дискретные частоты $n\omega_1\to\omega$, т. е. спектр из дискретного превращается в сплошной, а $\Delta(n\omega_1)\to d\omega_1$.

Интеграл под знаком суммы при $T\to\infty$ образует функцию, называемую спектральной плотностью и обозначается $F(j\omega)=\int\limits_{-\infty}^{\infty} f(t)e^{-j\omega t}dt.$

В реальных условиях существует только сплошной спектр импульсов. Амплитуды гармонических составляющих для последовательности импульсов значительно больше, чем амплитуда огибающей спектральной плотности для одиночного импульса. Однако нормами определен расчет защищенности по одному импульсу независимо от предыдущих и последующих. Поэтому в расчетных формулах введена операция деления на корень квадратный из частоты следования импульсов, а неверное определение этой частоты приводит к ошибочному результату.

В случаях, когда технические средства применяются для обработки информации ограниченного доступа, наибольшую актуальность имеют вопросы, связанные с информативными ПЭМИ и наводками информативных сигналов на токопроводящие цепи. Под ними понимают ПЭМИ и наводки, которые содержат сведения об обрабатываемой информации и могут быть перехвачены заинтересованными лицами. Характер ПЭМИ определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также материалами, из которых изготовлен корпус, и его конструкцией.

Согласно действующим нормативно-методическим документам, при проведении специальных исследований требуется измерять информативные ПЭМИ. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться при измерениях. Для того чтобы выделить информационные ПЭМИ, на исследуемом техническом средстве предусматривают специальные тестовые режимы его работы. Требования к тестам определяются в соответствующих ГОСТ и методиках.

В соответствии с методикой проведения специальных исследований технических средств по измерению их собственного электромагнитного излучения проводятся следующие операции:

1. Контролируемое устройство включается в тестовый режим.

2. На определенном расстоянии (обычно 0,5 м) от устройства устанавливаются поочередно антенны для приема электрической и магнитной составляющих поля, излучаемого анализируемым устройством (рис. 7.20).

3. Электрический сигнал с выхода антенны подается на вход приемно-регистрирующего измерительного устройства, с помощью которого по результатам измерений по определенной методике производится расчет опасных зон.

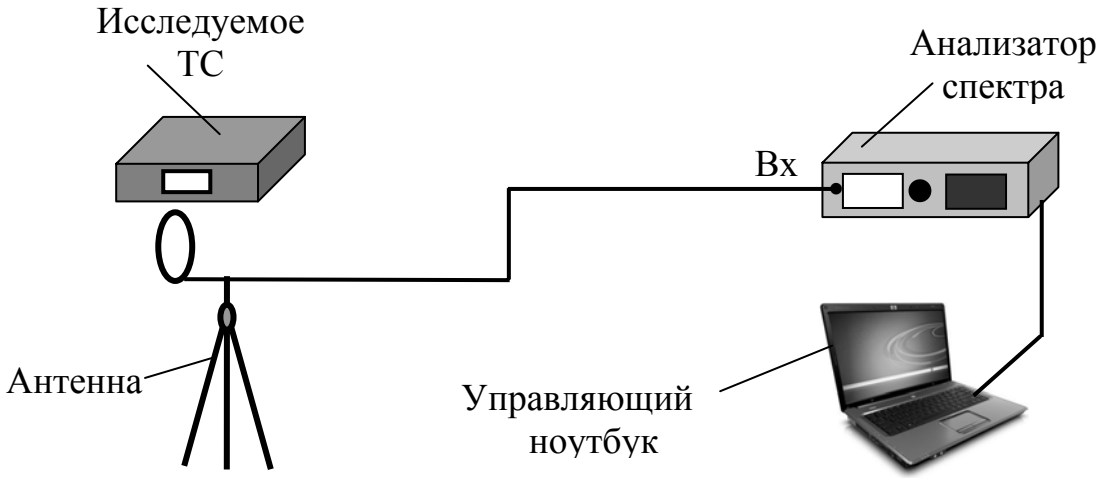


Рис. 7.20. Схема измерения ПЭМИ

Для исследования ПЭМИН видеоподсистемы ПЭВМ широко используется стандартный тест «Зебра», который обеспечивает вывод на экран определенного числа белых и черных горизонтальных полос, содержащих одинаковое число строк развертки монитора.

Наибольшую опасность утечки информации через ПЭМИН представляют узлы и устройства ПЭВМ, обрабатывающие информацию в последовательном коде. Информативные излучения в параллельном коде на сегодняшний день расшифровке не поддаются, так как через электромагнитные излучения невозможно определить принадлежность излученного импульса к какому-то разряду кода.

Исследованию на ПЭМИН подлежат следующие устройства:

- видеоподсистема;
- накопители на жестких и гибких дисках;
- устройства CD, CD-R, CD-RW, DVD, DVD-RW;
- клавиатура;
- последовательные порты;
- принтеры.

Применяемые средства измерения могут быть различными, но обязательно поверенными и имеющими сертификат Гостехкомиссии. Укажем лишь на программно-аппаратные комплексы «Легенда» и «Сигурд», выполненные на базе анализаторов спектра «R&S» и «IFR».

Эти комплексы имеют управляющую и расчетную программы, способны опознавать заданные тест-программами опасные сигналы по форме их огибающих. Оба комплекса в результате специсследований определяют опасные зоны R_2, r_1 и r_1' и формируют отчетный протокол. Эти исследования могут быть дополнены исследованиями по методу реальных зон.

Внешний вид основного рабочего экрана управляющей программы «Легенда» представлен на рис. 7.21.

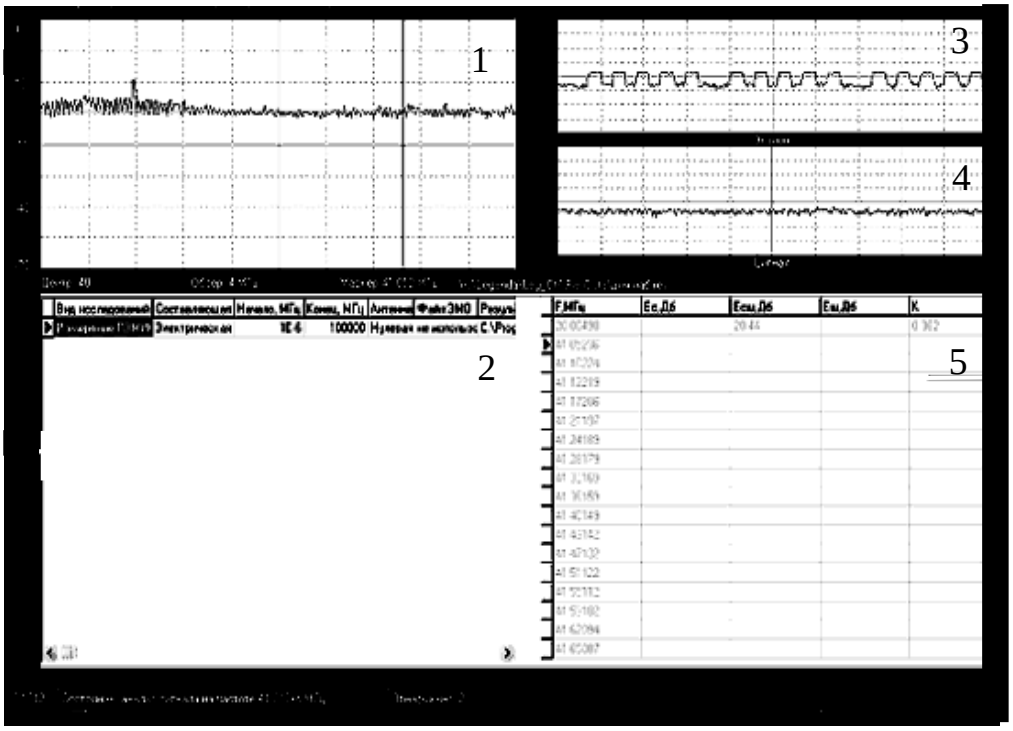


Рис. 7.21. Внешний вид экрана управляющей программы «Легенда»

На рис. 7.21 цифрами обозначены следующие элементы основного рабочего экрана (главного окна):

1 – окно спектра (отображается спектр сигнала для выбранного диапазона частот);

2 – таблица исследований (отображаются все программы исследований, которые будут выполнены в автоматическом режиме);

3 – окно эталона (осциллограмма найденного в полуавтоматическом режиме эталона тестового сигнала);

4 – окно сигнала (осциллограмма сигнала, который будет сравниваться с эталоном);

5 – рабочая таблица промежуточных результатов.

Вопросы для самопроверки

1. Что понимают под аттестацией объектов информатизации?
2. Какие документы являются нормативно-техническими при проведении аттестации объектов?
3. Какие полномочия предоставляет действующий «Аттестат соответствия»?
4. Какие объекты подлежат обязательной аттестации?
5. Какие оценки включает в себя разведдоступность объекта информатизации?
6. Из какого комплекса работ состоит проверка возможности утечки информации по техническим каналам?
7. Что представляют собой специальные проверки объекта защиты?
8. Комплекс каких мероприятий входит в специальные обследования объекта защиты?
9. Для чего производится легендирование специальных обследований выделенных помещений?
10. Из каких действий состоят поисковые мероприятия на объекте?
11. С какой целью проводятся специальные исследования?
12. Что является конечным результатом специальных исследований?
13. Какие объекты являются исследуемыми при проведении специальных исследований в области акустики?
14. На чем базируется действующая методика измерений акустических и виброакустических характеристик различных сред?
15. Перечислите типовые подсистемы современного программно-аппаратного комплекса для акустических измерений, например, «Спрут-7»?
16. Как определяется реальное затухание сигнала в виброакустическом канале утечки речевой информации?
17. Что понимают под прямым акустоэлектрическим преобразованием?
18. Что понимают под модуляционным акустоэлектрическим преобразованием?
19. Демаскирующие признаки сетевых акустических закладок.
20. Демаскирующие признаки проводной микрофонной системы подслушивания.
21. Демаскирующие признаки автономных некамуфлированных акустических закладок.
22. Демаскирующие признаки сетевых акустических закладок.
23. Демаскирующие признаки полуактивных акустических радиозакладок.
24. Демаскирующие признаки акустических и телефонных закладок с передачей на высокой частоте.
25. Причины возникновения паразитной генерации усилителей.
26. Почему опасно самовозбуждения усилителя?
27. Назовите наиболее простой способ выявления факта модуляции сигнала модуляционного акустоэлектрического преобразователя.

ЛИТЕРАТУРА

1. Хорев А.А. Технические каналы утечки акустической (речевой) информации. «Специальная техника» №1, 1998 г.

2. Хорев А.А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. «Специальная техника» №2, 1998 г.

3. Микроэлектронные устройства автоматики: Учеб. пособие для вузов / А.А. Сазонов, А.Ю. Лукичев, В.Т. Николаев и др.; Под ред. А.А. Сазонова. – М.: Энергоатомиздат, 1991. – 384 с.: ил.

4. Саликов В.Л. Приборы ночного видения: история поколений. Источник: журнал «Специальная техника», №2, 2000.

5. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М.: Российск. гос. гуманит. ун-т, 2002.

6. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.

7. Абалмазов Э.И. Направленные микрофоны: мифы и реальность // «Специальная техника» №4, 1996 г.

8. Иксар В. Современные способы перехвата информации. «Специальная техника» №2 1998 г.

9. Системы и комплексы технических средств местоопределения подвижных объектов. «Специальная техника», №3, 1998 г.

10. Петров Н.Н. Местоопределение подвижных объектов на основе спутниковых навигационных систем. // Журнал «Специальная техника», № 1, 1999.

11. Оленин Ю.А., Петровский Н.П. Системы безопасности. «Специальная техника», №29 1999г.

12. Ларин И. Быстроразвертываемые охранные системы. «Специальная техника», №4, 2000.

13. Введенский Б.С. Современные системы охраны периметров. «Специальная техника», №4, 1999.

14. Ллойд Дж. Системы тепловидения. М.: Мир, 1978.

15. Андреев С.П. ИК-пассивные датчики охранной сигнализации. Источник: журнал «Специальная техника» №1, 1998.

16. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безопасность: Информационно-справочное пособие. – М.: РАО «Газпром», 1994. – 170 с.

17. Специальная техника: Каталог. – М.: Гротек, 1996. – 83 с.

18. Специальная техника: Каталог. – М.: НПО «Защита информации», 1996. – 56 с.

19. Специальная техника: Каталог. – М.: Прогресстех, 1996. – 79 с.

20. Анюхин С.Г. Радиоволновые извещатели для охраны периметра. «Системы безопасности» №5 (59), 2004 г.

21. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Изд. Томского гос. ун-та систем управления и радиоэлектроники, 2004. – 197 с.

22. Волков В.Г. Наголовные приборы ночного видения. Источник: журнал «Специальная техника», №5, 2002.

23. Доценко С.М. Безопасность оптоволоконных кабельных систем // «Конфидент», №6, 1999.

24. Бландова Е.С. Помехоподавляющие изделия. Рекомендации по выбору и применению // Источник: журнал «Специальная техника», №2, 2001.

25. Прытко С.М., Топоровский Л.Н. Нелинейная радиолокация: принцип действия, область применения, приборы и системы //Системы безопасности. 1995, №6, с.52.

26. Вернигоров Н.С. Нелинейный локатор – эффективное средство обеспечения безопасности в области утечки информации // Конфидент. 1996, №1, с.67.

27. Вернигоров Н.С. Процесс нелинейного преобразования и рассеяния электромагнитного поля электрически нелинейными объектами // «Радиоэлектроника и Телекоммуникации» №3 (21), 2002 г.

28. Штейншлегер В.Б. Нелинейное рассеяние радиоволн металлическими объектами //Успехи физических наук. 1984, т.142, вып.1, с131.

29. Каталог ОАО «Ново». М., 1998г.

30. Вернигоров Н.С., Борисов А.Р., Харин В.Б. К вопросу о применении многочастотного сигнала в нелинейной радиолокации // Радиотехника и электроника. 1998. т.43, №1.

31. Теоретические основы электротехники. Том I. Основы теории цепей. Под ред. П.А. Ионкина. М.: Высш. школа, 1976.

32. Березанский Д.П. Металлодетекторы – устройства досмотра. Вопросы нормирования требований. «Специальная техника», №2, 1998 г.

33. http://kiev-security.org.ua/box/7/5.shtml

34. Томас Харви Джонс. Обзор технологий нелинейной локации. «Конфидент», №3, 1999 г.

35. Никольский В.В. Теория электромагнитного поля. Уч. пособие – М.: Изд-во «Высшая школа», 1964. – 384 с.

36. Электроакустика и звуковое вещание: Учебное пособие для вузов / И.А. Алдошина, Э.И. Вологдин, А.П. Ефимов и др.; Под ред. Ю.А. Ковалгина. – М.: Горячая линия – Телеком, Радио и связь, 2007. – 872 с.

37. Сапожков М.А. Электроакустика. – М.: Связь. 1978

38. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил. ISBN 5-93517-204-6.

39. Инженерно-техническая защита информации: учеб. Пособие для студентов, обучающихся по специальностям в обл. информ. безопасности/ А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

40. Григорьев С.В. Оптимизированная по спектру шумовая помеха // Защита информации Конфидент. – № 4. – 2003.

41. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – № 4. – 2000. – С. 39–45.

42. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат. 1962.

43. Ю.Ю. Орлов, А.В. Столяренко, Л.И. Громовенко, О.Ю. Жариков. Принцип действия и особенности функционирования инфракрасных пассивных охранных извещателей. Источник: http://www.bcm.com.ua

44. http://www.profinfo.ru/catalog/r33/118.html

45. http://www.spymarket.com/prod/recom.shtml

46. http://www.info-protect.ru/product/362.html

47. http://www.nppecomp.ru/rus/dok/sdke.htm

48. http://mascom.ru/article255.asp.htm

49. Мобильные новости. 8(48), 2004 г.

50. http://www.sbchel.ru/content/it/po/secretnet/

51. http://law.itdom.biz/attest.htm

52. А.А. Хорев. Оценка эффективности защиты вспомогательных технических средств. // Специальная техника. – № 2, №3. – 2007.

53. www.vizir-company.com

54. www.yukonoptics.ru

55. www.vsebinokli.ru

56. www.bnti.ru

57. www.laborkomplekt.ru

58. raznoe1.videomix.ru

59. www.top-mag.ru

60. www.bnti.ru

61. www.pdamix.ru

62. info-protect.ru

63. www.infosecur.ru

64. www.brandcenter.ru

65. www.dignum.ru

ЛАБОРАТОРНЫЕ РАБОТЫ

Лабораторная работа №1

СТАТИСТИЧЕСКИЙ АНАЛИЗ ЗАГРУЗКИ ЗАДАННОГО РАДИОДИАПАЗОНА И ОБНАРУЖЕНИЕ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ В ЗАЩИЩАЕМОМ ПОМЕЩЕНИИ

1. Цель работы

Изучить методы статистического анализа заданного радиодиапазона и обнаружения радиомикрофонных закладок с помощью компьютеризированных комплексов RS turbo, RS turbo Mobile-L.

2. Методы поиска радиозакладок

Для обнаружения радиозакладок применяют индикаторы электромагнитного поля, частотомеры, нелинейные локаторы, рентгенотелевизионную аппаратуру и специальные сканирующие приемники. С их помощью осуществляется поиск и фиксация рабочих частот радиозакладок, а также определяется их местонахождение.

Если радиозакладки выключены в момент поиска и не излучают сигналы, то для их поиска, а также для поиска микрофонов подслушивающих устройств и минимагнитофонов, применяют специальную рентгеновскую аппаратуру и нелинейные локаторы, излучения которых проникают сквозь стены, потолки, пол, мебель, портфели, утварь – в любое место, где могут быть спрятаны радиозакладка, микрофон, магнитофон.

В тех случаях, когда нет приборов либо нет времени на поиск радиозакладок, можно пользоваться генераторами помех для подавления закладочных устройств.

К средствам оперативного контроля, то есть средствам обнаружения факта использования радиозакладки, а иногда и ее локализации, относятся индикаторы или детекторы поля, частотомеры и некоторые поисковые приемники. Основное их преимущество – способность выявлять источники излучения или передающие устройства независимо от типа применяемой в них модуляции. Принцип поиска заключается в выявлении максимума уровня излучения в помещении.

3. Описание комплексов

Комплекс «RS turbo Mobile-L»

Компьютеризированный комплекс «RS turbo Mobile-L» (рис. 1) предназначен для быстрого обнаружения, идентификации, определения местоположения (локализации) и нейтрализации подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, проводным линиям и в оптическом ИК-диапазоне.

Рис. 1. Комплекс «RS turbo Mobile-L»

В состав комплекса «RS turbo Mobile-L» входят:

− радиоприемное устройство на базе AR5000 с встроенными контроллером RS turbo (или RS digital) и конвертором RS/L plus;

− антенна RS/A;

− двухканальная акустическая система;

− портативный персональный компьютер (ноутбук) с операционной системой Windows XP;

− управляющая программа.

Комплекс «RS turbo Mobile-L» имеет удобные программные средства накопления, обработки, анализа и хранения данных, регистрации демодулированных сигналов и идентификации источников излучений. Основная задача управляющей программы комплекса – облегчить оператору анализ поступающей информации о многочисленных источниках излучений. В процессе просмотра заданных диапазонов и обработки полученных данных программа составляет списки с параметрами и классификационными признаками обнаруженных сигналов. Затем, с помощью средств анализа программы оператор может детально исследовать характеристики интересующего сигнала, например, его спектр, гармонический состав или реакцию на импульсы акустического зондирования и получить необходимую информацию для принятия обоснованного решения о наличии в помещении подслушивающих устройств.

Сохраняя все положительные качества изделий серии Turbo (компактность, надежность, простоту освоения и эксплуатации), эта система отли-

чается целым рядом новых возможностей и, прежде всего, скоростью работы. Так время полного обзора радиодиапазона до 2,6 ГГц при отсутствии априорных данных о его загрузке составляет от 0,5 до 2-х мин. Оболочка управляющей программы работает в среде Windows 95/98/NT/2000/XP.

Комплекс «RS turbo Mobile-L» в автоматическом режиме с высокой достоверностью выявляет в контролируемом помещении радиомикрофоны и телефонные радиопередатчики, с достаточной точностью указывает местоположение обнаруженных микрофонов с обычной частотной модуляцией.

Комплекс «RS turbo»

Комплекс «RS turbo» выполняет все функции комплекса «RS turbo Mobile-L», однако позволяет сканировать радиодиапазон вплоть до 12 ГГц с дополнительным конвертером. С помощью конвертера RS/L комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне от 0,6 кГц до 10 МГц, а также в инфракрасной части оптического диапазона. Одновременно комплекс с достаточной точностью указывает местоположение обнаруженных радиомикрофонов с обычной частотной модуляцией, а при необходимости нейтрализует их излучения с помощью программируемых генераторов сигналов RS/N.

Для выполнения базовых операций поиска подслушивающих устройств в радиоканале достаточно подключить к контроллеру персональный компьютер, сканирующий радиоприемник и двухканальную акустическую систему. Комплекс «RS turbo» работает со сканерами AR5000, AR8600 и AR8200 японской фирмы AOR Ltd. Для управления может использоваться любой компьютер с операционной системой Windows 95/98/2000/NT и одним свободным последовательным портом RS232. В случае необходимости конфигурацию системы легко расширить с помощью дополнительных устройств, разработанных для комплексов радиоконтроля. В частности, для анализа проводных и оптических каналов используется конвертер RS/L, а для нейтрализации выявленных источников радиоизлучений – программируемый генератор RS/N (до 1800 МГц). С помощью антенного коммутатора RS/K комплекс может контролировать радиообстановку с помощью нескольких антенн, предназначенных для различных диапазонов или установленных в пространственно разнесенных помещениях. Контроллеры акустических систем RS/Z используются для обнаружения и определения местоположения радиомикрофонов методом акустического зондирования в удаленных помещениях.

Общая схема соединений аппаратуры комплекса «RS turbo»: компьютера, сканирующего радиоприемника, местной акустической системы и контроллера показана на рис. 2. На лицевой стороне корпуса контроллера «RS turbo» находятся светодиод, индицирующий наличие напряжения питания, которое поступает от собственного блока питания, телефонный разъём для

подключения к последовательному порту управления приемником, телефонный разъём шины I2C для подключения дополнительных периферийных устройств, а также гнездо для подключения акустических колонок «Speaker». На задней стороне контроллера находятся разъём для подключения последовательного интерфейса RS232 компьютера (COM-порт), гнездо круглого разъема питания 12 вольт и разъём CP-50 для подключения выхода промежуточной частоты приемника AR8200. К контроллеру поставляется комплект специальных соединительных кабелей, различных для каждого типа приемников.

Рис. 2. Комплекс «RS turbo»

Сканирование

Сканирование – это базовая операция, которая предшествует обнаружению, классификации и идентификации источников излучений (сигналов). В процессе сканирования выявляются занятые участки исследуемого частотного диапазона и оцениваются спектры присутствующих в нем сигналов. Частота настройки сканирующего приемника изменяется дискретно с фиксированным шагом 8 МГц и на каждом шаге вычисляемый контроллером «RS turbo» результат измерений уровней, принимаемых во всем спектре сигналов, заносится в компьютер. В анализаторе «RS turbo» быстрое сканирование выполняется с широким (200 кГц) или узким (12,5 кГц) шагом. По результатам сканирования компьютер формирует спектральную панораму исследуемого диапазона, в которой каждому значению частоты настройки соответствует измеренный спектр сигнала.

Операции сканирования выполняются в порядке их размещения в списке операций задания. Это дает возможность в первую очередь просматривать те участки спектра, где вероятность найти излучения несанкционированных источников выше. Один частотный диапазон можно включать в задание несколько раз, чтобы реализовать различные алгоритмы идентификации и классификации излучений.

Выполнив один цикл сканирования, программа составляет таблицу, в которой каждому значению частоты настройки ставится в соответствие измеренный последовательным анализатором контроллера «RS turbo» спектр сигналов в полосе анализа 8 МГц, снятый для сигналов, превышающих заданный порог, с разрешением 12.5 кГц. Эта таблица называется спектральной панорамой. Программа комплекса «RS turbo» позволяет формировать спектральные панорамы с учетом данных, полученных в ходе текущего и любого числа предшествующих циклов сканирования. После выполнения первого цикла сканирования таблица спектральной панорамы сохраняется в памяти компьютера. На следующем цикле формируется новая (текущая) таблица, а значения уровней в таблице предыдущей панорамы модифицируются в соответствии с выбранным методом обработки:

−обновление (в таблицу записывается новое значение, а старое стирается);

−накопление (в таблицу записывается больший из двух уровней);

−усреднение (в таблицу записывается среднее двух уровней).

Первый из перечисленных методов обычно используется в процессе обнаружения излучений, а следующие два – для сбора данных, характеризующих обстановку в заданных диапазонах при продолжительных наблюдениях со статистической обработкой результатов измерений. Накопление максимальных значений обеспечивает наиболее полный учет всех излучений, появлявшихся за время наблюдения. Накопление средних значений позволяет при большом числе циклов сканирования свести к нулю уровни

случайных сигналов, например, импульсных помех. Текущая панорама отображается на экране зеленым цветом и показывает уровни, измеренные в текущем цикле сканирования.

Данные, полученные в результате обработки уровней предшествующих циклов сканирования, отображаются красным цветом и располагаются на заднем плане. В любой момент после остановки сканирования таблица панорамы, отражающая результаты выполненных циклов сканирования, может быть сохранена в виде файла (файл панорамы спектра, расширение .pan) с заданным программой или пользователем именем. Спектральные панорамы, характеризующие обстановку в заданном диапазоне частот, называются диаграммами загрузки диапазона. Такие панорамы на экране отображаются синим цветом и используются в качестве фона для обнаружения «неизвестных» излучений.

При необходимости данные, отражающие результаты предшествующих циклов сканирования, могут быть удалены из списка командой очистки. При этом в исходную таблицу панорамы записываются нулевые уровни. Если программа работает с несколькими заданиями, то таблица уровней составляется и модифицируется для каждого из них. При этом на экране отображаются панорамы спектров активного задания. В процессе анализа проводных линий с помощью конвертора «RS/L plus» текущий спектр зеленого цвета выводится на экран на фоне спектра красного цвета, полученного на предыдущем цикле.

Для повышения скорости работы комплекс «RS turbo» выполняет сканирование с помощью последовательного анализатора спектра с разрешением 12,5 КГц с шагом 8 МГц. После запуска сканирование ведется с указанным шагом по сетке частот. Начальная и конечная частоты указанного в задании диапазона заменяются ближайшими частотами этой сетки. На каждом шаге контроллер «RS turbo» измеряет уровни принимаемых сигналов, т.е. снимает спектр на широкополосном выходе промежуточной частоты приемника, и передает данные в компьютер.

Обнаружение

Обнаружение – базовая операция выявления всех радиоизлучений (сигналов), уровень которых в заданном диапазоне превосходит установленное в задании пороговое значение (порог обнаружения). В процессе обнаружения программа оценивает параметры сигнала: ширину спектра, максимальный уровень, несущую частоту, а также классифицирует обнаруженные излучения, распределяя их по группам в соответствии с определенными признаками. Обнаруженные излучения автоматически классифицируются программой RS turbo по следующим признакам:

− «известные» и «неизвестные»;

− «обнаруженные ранее» и «вновь появившиеся»;

− «стандартные» и «нестандартные».

Анализ

Операции анализа необходимы для выявления среди множества обнаруженных сигналов «опасных» излучений, которые могут быть созданы передатчиками подслушивающих устройств. Идентификация (опознавание) сигналов подслушивающих устройств в программе «RS turbo» выполняется автоматически или в ручном режиме с помощью следующих операций:

− анализ гармонического состава излучений;

− корреляционный анализ откликов на акустические импульсы;

− спектральный анализ;

− временной и спектральный анализ сигналов на выходе демодулятора.

Кроме того, в процессе анализа откликов на импульсы акустического зондирования программа измеряет расстояния от колонок акустической системы комплекса до микрофона и определяет местоположение микрофона в помещении (локализация источника излучения).

4. Задание для работы

4.1. Ознакомиться с видами радиозакладок и изучить методы их обнаружения.

4.2. Изучить работу комплексов в режиме обнаружения радиозакладок.

4.3. Произвести настройку программы для работы в режиме «Радио». Выполнить один или несколько циклов сканирования заданного радиодиапазона. Обнаружить излучения без учета априорных данных за один цикл сканирования.

4.4. Посмотреть и проанализировать списки обнаруженных сигналов.

4.5. Для интересующего сигнала выполнить:

− спектральный анализ сигналов излучений;

− анализ гармонического состава сигналов излучений;

− корреляционный анализ откликов на акустические импульсы.

4.6. Выявить наличие радиозакладного устройства в контролируемом помещении.

5. Порядок выполнения работы

5.1. Создать отдельное задание с несколькими операциями сканирования радиодиапазона. Для этого в меню «Настройки» выбрать «Установка параметров». В окне «Настройка программы» щелкнуть на закладку «Задание» (рис. 3). Выбрать режим «Радио».

5.2. В окне «Диапазон» установить диапазон сканирования частот от 10 до 1000 МГц, желаемое число циклов сканирования и заданный порог 50 при выключенном аттенюаторе. Щелкнуть по кнопке ОК (закрыть окно).

5.3. Запустить сканирование нажатием кнопки «Старт». Провести простое сравнение по масштабной сетке окна спектральной панорамы составляющих измеренного с разрешением 12,5 кГц спектра сигнала с указанным в задании порогом.

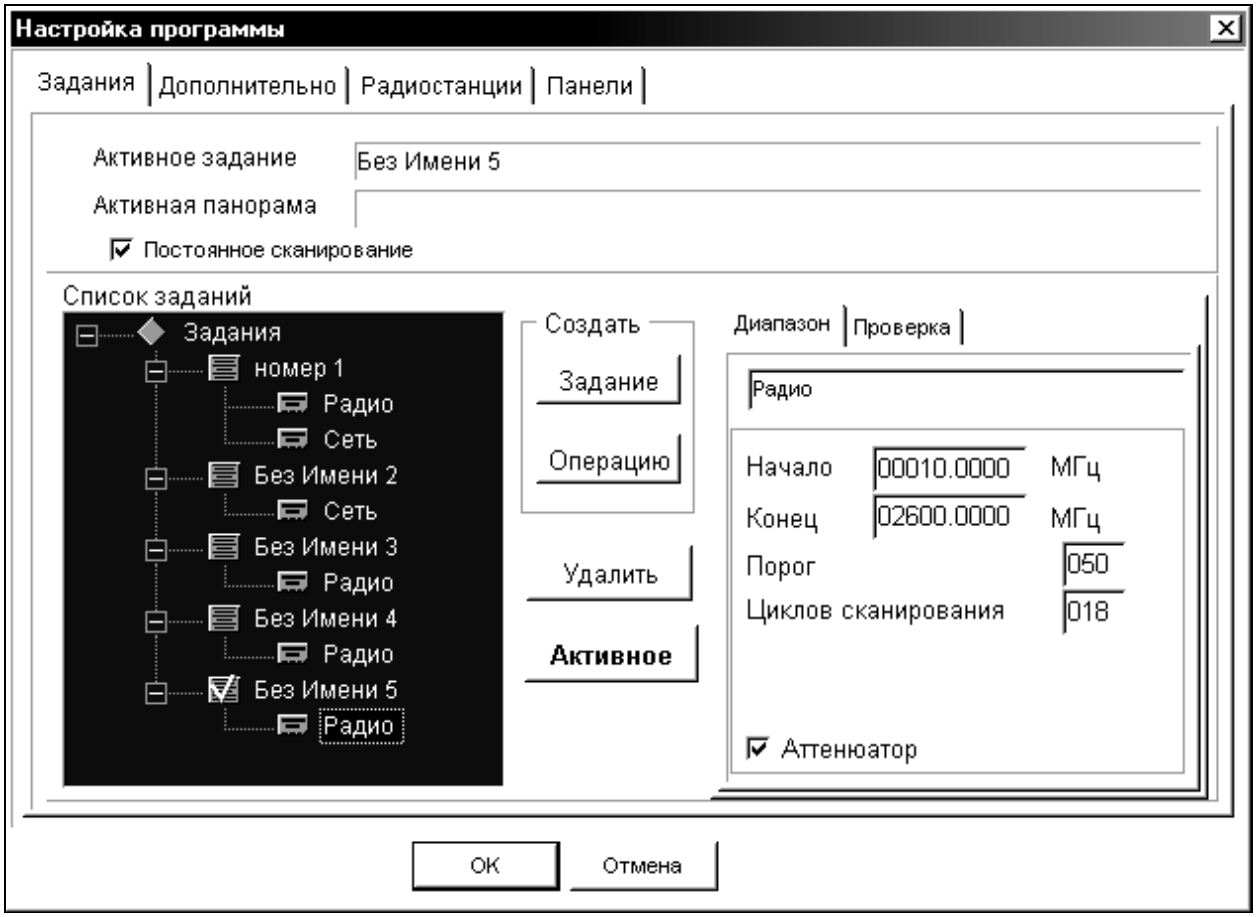


Рис. 3. Окно «Настройка программы»

5.4. Зафиксировать уровень сигналов, превышающих заданный порог. Программа запоминает частоту и уровень сигналов излучений. Данные о частоте и уровне сигналов, обнаруженных с помощью входящего в состав комплекса конвертора RS/L plus, заносятся в список сигналов. В центре окна монитора размещается экран панорамного отображения спектров. Вертикальная ось экрана панорамного отображения спектров отражает интенсивность принимаемого сигнала в децибелах относительно уровня шума приемника.

Горизонтальная ось соответствует частоте диапазона сканирования. Над экраном панорамы спектра находятся закладки «Радио», «Сеть» и «Панорама» (рис. 4).

Закладка «Радио» позволяет наблюдать процесс сканирования радиодиапазонов и текущие спектральные панорамы, полученные после выполнения заданных циклов сканирования, а закладка «Панорама» используется для просмотра файлов спектральных панорам.

Отображение спектральной панорамы в закладках «Радио» и «Панорама» ведется с разрешением 200 кГц. Линейка горизонтальной прокрутки в закладках «Радио» и «Панорама» позволяет просматривать весь рабочий диапазон сканера участками по 10, 100, 500 или 1000 МГц в зависимости от выбранного масштаба отображения по оси частот (полосы обзора).

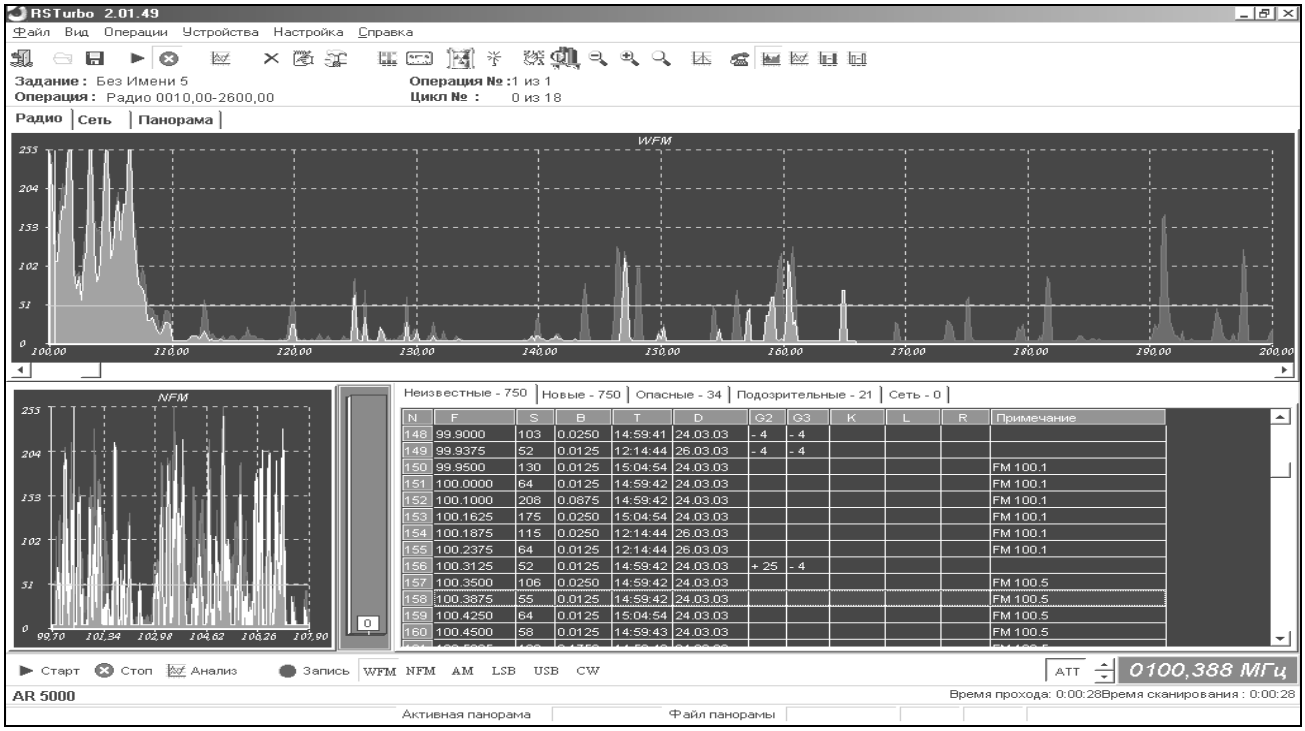


Рис. 4. Окно панорамного отображения спектров

Ниже окна спектральной панорамы (при выборе закладок «Радио» или «Панорама») помещается окно детального анализа спектра с полосой обзора, которая автоматически изменяется в процессе сканирования в зависимости от ширины спектра обнаруженного сигнала. Это окно отображает текущие спектры излучений с разрешением 12,5 кГц. Справа находится вертикальный (столбцовый) индикатор уровня принимаемого сигнала с дополнительной цифровой индикацией и окно списков обнаруженных частот. Кнопки «Старт» и «Стоп» в нижней части экрана запускают и останавливают процесс сканирования, а кнопка «Анализ» вызывает окно для выполнения операций идентификации и классификации излучений на выделенной в списке частоте. Рядом с кнопкой «Анализ» находятся кнопки выбора типа демодулятора сканера и управления аттенюатором, а также индикатор частоты настройки приемника с кнопками пошагового изменения частоты настройки сканера.

В нижней части основного окна находятся две строки состояний. В первой отражается тип сканера, с которым работает комплекс, и время, затраченное на выполнение текущей операции сканирования. Во второй строке появляются поясняющие сообщения о функциях кнопок окна, а также имена файлов спектральной панорамы, которые используются в качестве диаграммы загрузки диапазона при классификации сигналов (Активная панорама) и загружены для просмотра в закладке «Панорама» (Файл панорамы).

5.5. Настроить приемник на выбранную частоту и выполнить анализ радиоизлучения. Настраивать приемник удобно с учетом полученных дан-

ных о радиообстановке. Текущая частота настройки приемника в основном окне программы отражается цифровым индикатором и положением курсоров в окнах спектральной панорамы.

Для изменения частоты настройки откройте закладку «Радио», установите в окне спектральной панорамы удобный масштаб отображения по оси частот (полосу обзора) и найдите интересующий участок спектра с помощью линейки прокрутки. Щелчок мыши в интересующей области диапазона переместит курсор и настроит приемник на ближайшую частоту из 200-кГц сетки. Одновременно программа включает широкую полосу пропускания приемника (WFM). Точная настройка выполняется мышью в нижнем окне детального анализа спектра с шагом 12,5 кГц. При этом приемник переключается в узкополосный режим NFM. Для перестройки частоты на несколько шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Если включена (нажата) кнопка WFM, щелчок по кнопкам увеличить/уменьшить переместит курсор в верхнем окне спектральной панорамы соответственно вправо или влево и перестроит приемник на 200 кГц. Если нажата кнопка NFM, двигаться будет курсор нижнего окна спектральной панорамы и шаг перестройки составит 12,5 кГц. Кроме того, произвольное значение частоты настройки можно ввести с клавиатуры, щелкнув левой кнопкой мыши по индикатору частоты настройки основного окна.

В окне ввода набрать требуемое значение частоты в МГц и щелкнуть по кнопке OK. Введенное значение частоты программа приведет к ближайшему значению из сетки частот сканирования.

5.6. Провести анализ подозрительных и опасных радиоизлучений.

В задании предусмотрено сканирование заданного диапазона с анализом гармонического состава обнаруженных излучений (обнаружение 2-й гармоники, обнаружение 3-й гармоники, одновременное обнаружение 2-й и 3-й гармоник). Программа, обнаружив сигнал и измерив его несущую частоту f, настраивает приемник на частоту $2f$ и/или $3f$, измеряет уровни гармоник при максимальной чувствительности (отключив аттенюатор) и сравнивает их с пороговым значением. В случае превышения порога программа принимает решение о наличии излучения на гармониках основной частоты и в списках обнаруженных сигналов в графах гармоник (G2 и G3) указывается измеренный уровень с пометкой «+». Если гармоника не обнаружена – уровень указывается с пометкой «–».

Если проверка не выполнялась, например, из-за того, что частота гармоники лежит вне рабочего диапазона сканера, – графа остается пустой. Обнаружив одну из гармоник, программа помещает данные о сигнале в список «подозрительных» излучений. Если обнаружены обе гармоники – в список «опасных» сигналов.

В процессе сканирования радиодиапазонов на экране панорамного обзора будут отображаться 100-МГц участки с разрешением 200 кГц, а на экране детального анализа – спектр последнего обнаруженного сигнала (сигналов) с разрешением 12,5 кГц. Кроме того, программа в соответствии с заданием выполняет операции автоматической классификации и идентификации обнаруженных источников излучений. При сканировании радиодиапазонов в системе «RSturbo» можно использовать любую комбинацию из перечисленных ниже методов идентификации и классификации сигналов.

Провести классификацию сигналов на «известные» и «неизвестные» с использованием диаграмм загрузки радиодиапазона. Диаграммы загрузки характеризуют внешние и внутренние излучения при продолжительных наблюдениях со статистической обработкой результатов измерений. Обнаружение излучений без учета априорных данных позволяет выявить и занести в список все без исключения источники, мощность которых в точке приема больше заданной. Однако полученный список обнаруженных сигналов в большинстве случаев оказывается слишком обширным. Необходимо сократить его, исключив те излучения, которые были обнаружены ранее, проверены и признаны не представляющими опасность. После необходимой проверки источники этих излучений можно считать «известными» в том смысле, что они регулярно присутствуют в эфире и не представляют опасности для контролируемого объекта. Классификация сигналов на «известные» и «неизвестные» позволяет оставить в списке обнаруженных излучений только те, которые не содержатся в диаграмме загрузки.

Если обнаружение планируется выполнять с классификацией излучений на «известные» и «неизвестные», необходимо использовать нужный файл диаграммы загрузки. Алгоритм обнаружения и классификации выглядит следующим образом. Выделив в цикле сканирования участок группы смежных частот, превышающих порог обнаружения, и определив максимальные уровни в каждой из них, программа проверяет, попадает ли текущий максимум каждой группы в одну из полос «известного» излучения, присутствующего в диаграмме. Полоса известного излучения определяется числом уровней в группе частот, превышающих порог обнаружения (рис. 5). Если ответ положительный, программа считает излучение известным. В противном случае принимается решение об обнаружении «неизвестного» излучения, данные о котором заносятся в список «неизвестных» излучений с учетом результатов обнаружения на предыдущих циклах сканирования.

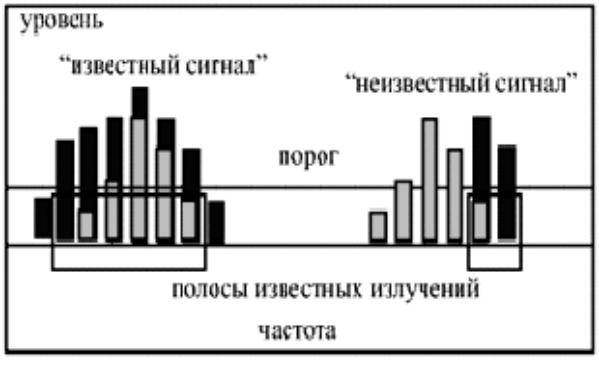


Рис. 5. Классификация сигналов на «известные» и «неизвестные»

5.7. Провести классификацию сигналов на «вновь появившиеся» и «обнаруженные ранее» на предыдущих циклах сканирования с использованием текущей спектральной панорамы.

Если в задании предписано выполнение нескольких циклов сканирования или панорама спектра предыдущего сеанса работы была сохранена, обнаружение выполняется следующим образом. Выделив в каждом цикле сканирования участка группы смежных частот, превышающих порог обнаружения, и определив максимальные уровни в каждой из них, программа проверяет, попадает ли текущий максимум каждой группы в полосу одного из сигналов, обнаруженных на предыдущем цикле сканирования (рис. 6).

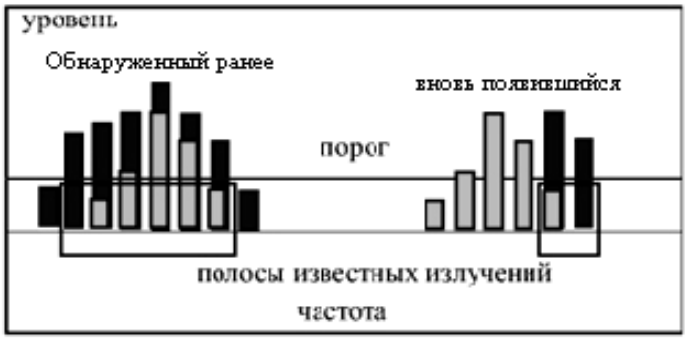


Рис. 6. Классификация сигналов на «обнаруженные ранее» и «вновь появившиеся»

Полоса излучения, обнаруженного на предыдущем цикле сканирования, определяется числом уровней в группе частот, превышающих порог. Если ответ отрицательный, то принимается решение об обнаружении «нового» излучения, данные о котором заносятся в списки. В противном случае программа считает излучение уже обнаруженным. В результате размер списков обнаруженных сигналов существенно сокращается. Кроме того, отдельный список «новых» излучений значительно упрощает контроль текущих изменений радиообстановки. Действительно, если очистить список «новых» излучений, то в последующих циклах сканирования в него будут попадать только вновь обнаруженные сигналы. Остальную информацию можно найти в списке «неизвестных» излучений, который содержит все сигналы, обнаруженные с момента последней очистки спектральной панорамы.

5.8. Провести акустическое зондирование. Кнопкой «Анализ» или командой «Анализ меню Операции» вызвать окно анализа обнаруженных сигналов, в названии которого указывается частота анализируемого сигнала. В этом окне выбирается закладка «Звуковой тест». В верхней части закладки отображается реверберационная картина помещения, для просмотра которой можно воспользоваться линейкой прокрутки (рис. 7).

Измерить расстояние от звуковой колонки до некоторой точки, например, одного из импульсов, можно, указав на него курсором мыши. При этом значение расстояния в метрах отображается в правом верхнем углу экрана реверберационной картины. В нижней части закладки отображается корреляционная функция отклика, расстояния от звуковых колонок до

микрофона и значение коэффициента корреляции. Чтобы выполнить акустический тест, необходимо из нужного списка выбрать интересующий сигнал, установить полосу приема (NFM или WFM), указать число циклов (импульсов) звукового зондирования и нажать кнопку с изображением левой или правой колонки. При повторном выполнении теста предыдущая реверберационная картина стирается. Закончив анализ, щелкните по кнопке «Выход».

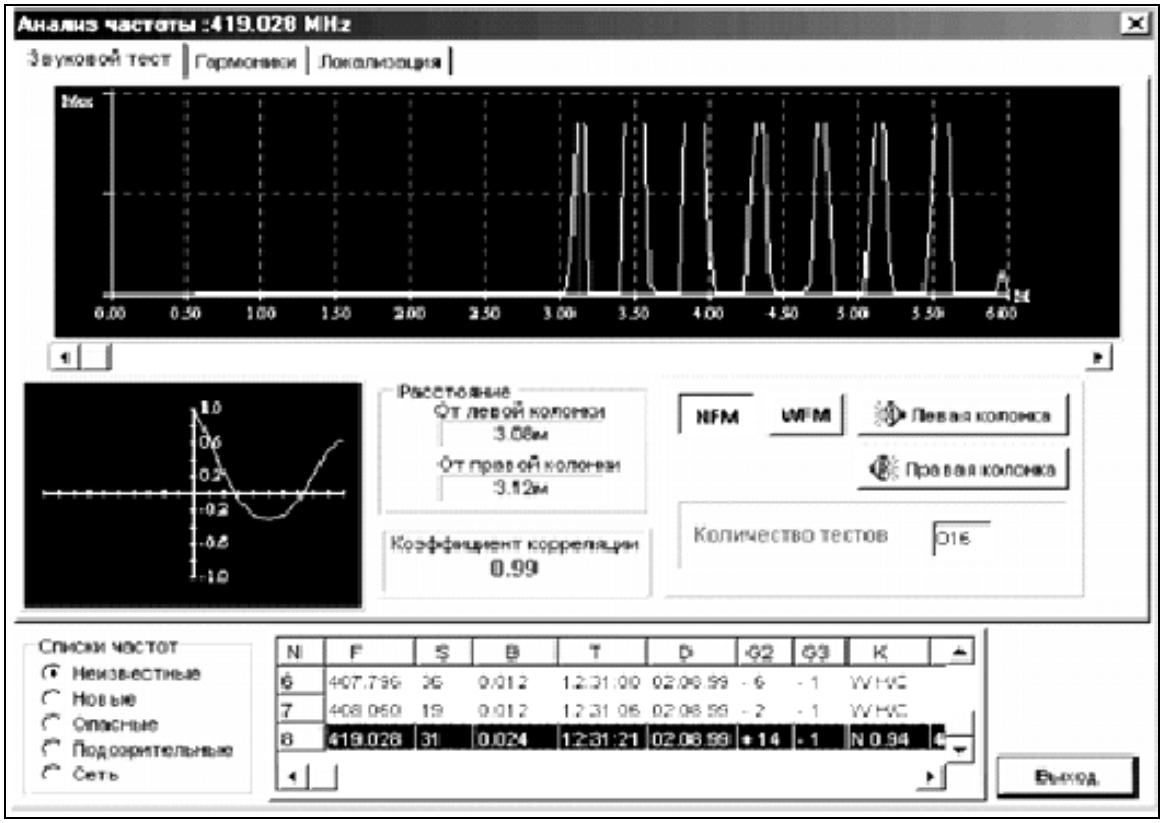


Рис. 7. Окно звукового зондирования

5.9. Провести акустическое зондирование в автоматическом режиме. Если в задании предусмотрено сканирование с идентификацией радиомикрофонов методом акустического зондирования, программа, обнаружив сигнал и измерив его несущую частоту и ширину спектра, выполняет на несущей частоте акустический тест, включив узкую полосу пропускания (режим NFM).

Звуковые импульсы, число которых задается при настройке, излучаются левой колонкой акустической системы. После этого вычисляется коэффициент корреляции отклика и сравнивается с порогом, величина которого составляет 0,6. Если порог превышен, программа принимает решение об идентификации сигнала радиомикрофона. Для повышения скорости работы в автоматическом режиме звуковой тест выполняется с высокой частотой повторения акустических импульсов.

Полученные результаты (коэффициент корреляции, полоса пропускания, расстояния от радиомикрофона до колонок акустической системы) заносятся в список «опасных» излучений. Если при тестировании через первую колонку порог не превышается, программа повторяет тест с помощью второй колонки, а затем – в широкой полосе пропускания приемника (режим WFM). Если и в этом случае результаты звукового теста отрицательны, в списки «неизвестных» и «новых» излучений заносятся только значения коэффициента корреляции. При высокой частоте повторения акустических импульсов из-за реверберации измерение расстояний от колонок до радиомикрофона иногда выполняется с ошибками. Уточнить расстояния можно, выполняя акустический тест в ручном режиме.

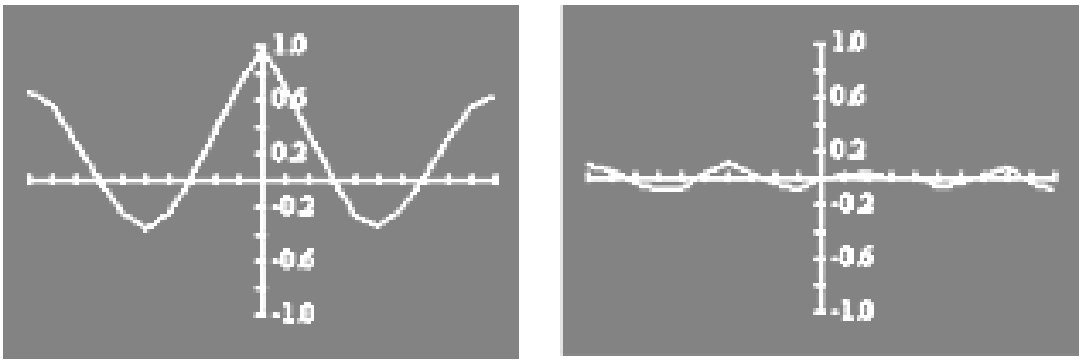
5.10. Провести анализ излучений методом акустического зондирования в ручном режиме. В ручном режиме оператор имеет возможность выполнять акустический тест отдельно для левой и правой колонок, наблюдать реверберационные картины помещения, корреляционную функцию отклика, выбирать число звуковых импульсов, переключать полосу пропускания приемника (NFM, WFM). Для проведения акустического теста необходимо настроить приемник на несущую частоту интересующего излучения, выбрав нужную запись из списка обнаруженных сигналов или указав значения частоты с клавиатуры, указать полосу пропускания, число зондирующих импульсов и нажать кнопку левой или правой колонки. В ручном режиме программа снижает частоту повторения акустических импульсов для того, чтобы избежать реверберационых помех и повысить достоверность измерений дальности. Окно реверберационной картины помещения отображает интенсивность принятого импульсного сигнала в зависимости от времени, которое пересчитано в расстояние. Вертикальная шкала градуируется в относительных единицах, а горизонтальная – в метрах. Линейка прокрутки окна позволяет наблюдать отклики на дистанциях до 30 м.

Пользователь может также измерить расстояние до любого импульса, указав на него курсором. Автокорреляционная функция отклика, отражающая зависимость коэффициента корреляции от времени служит дополнительным инструментом, облегчающим процесс идентификации сигналов в сомнительных случаях.

На рис. 8 изображены корреляционные функции откликов для радиомикрофона и внешней станции. Как известно, форма корреляционной функции одиночного импульса близка к треугольной. Присутствие нескольких отраженных импульсов в отклике вызывает появление боковых выбросов корреляционной функции той же формы.

Акустическое зондирование позволяет автоматически идентифицировать излучения только тех подслушивающих устройств, в которых используется стандартная узкополосная или широкополосная частотная модуляция. Если обнаружен сигнал с иными параметрами модуляции или

цифровым кодированием (с поднесущими, с инверсией спектра, цифровой модуляцией и т.д.), значение коэффициента корреляции обычно не достигает порогового уровня. Вместе с тем оператор может идентифицировать такой сигнал, повторив операцию акустического зондирования несколько раз. В этом случае коэффициент корреляции будет небольшим (от 0,2 до 0,4 в зависимости от типа устройства), но относительно стабильным, тогда как для внешних станций его значение случайно изменяется в пределах от -0,3 до +0,3. Сказанное не относится к микропередатчикам с цифровой модуляцией, в которых применяются специальные методы декорреляции акустического и модулирующего сигналов (скремблирование цифрового потока).



а *б*

Рис. 8. Корреляционные функции откликов: *а* – для радиомикрофона; *б* – для внешней станции

5.11. Провести анализ спектра. Анализатор спектра вызывается инструментальной кнопкой основного окна программы или командой «Спектр меню Операции». Полоса обзора анализатора отсчитывается вверх и вниз относительно центральной частоты. Значение полосы обзора соответствует ширине тракта ПЧ приемника – 8 МГц. Значение центральной частоты устанавливается программой при выделении записи в одном из списков обнаруженных сигналов или вводится оператором. В верхней части окна находятся позиции выбора состояния аттенюатора и полосы анализа (12,5 кГц или 200 кГц). После ввода этих параметров необходимо щелкнуть мышью по кнопке «Установить».

В нижней части окна находится выпадающий список выбора режима обработки спектральных составляющих в последовательных циклах обзора. В режиме обновления текущее значение заменяет предшествующее, в режиме накопления выбирается максимальное из этих двух значений, а в режиме усреднения – среднее. Щелчок по кнопке «Старт» включает циклический режим анализа спектра в заданной полосе обзора. Спектральные составляющие текущего цикла обзора отражаются зеленым цветом, предыдущего – красным (рис. 9).

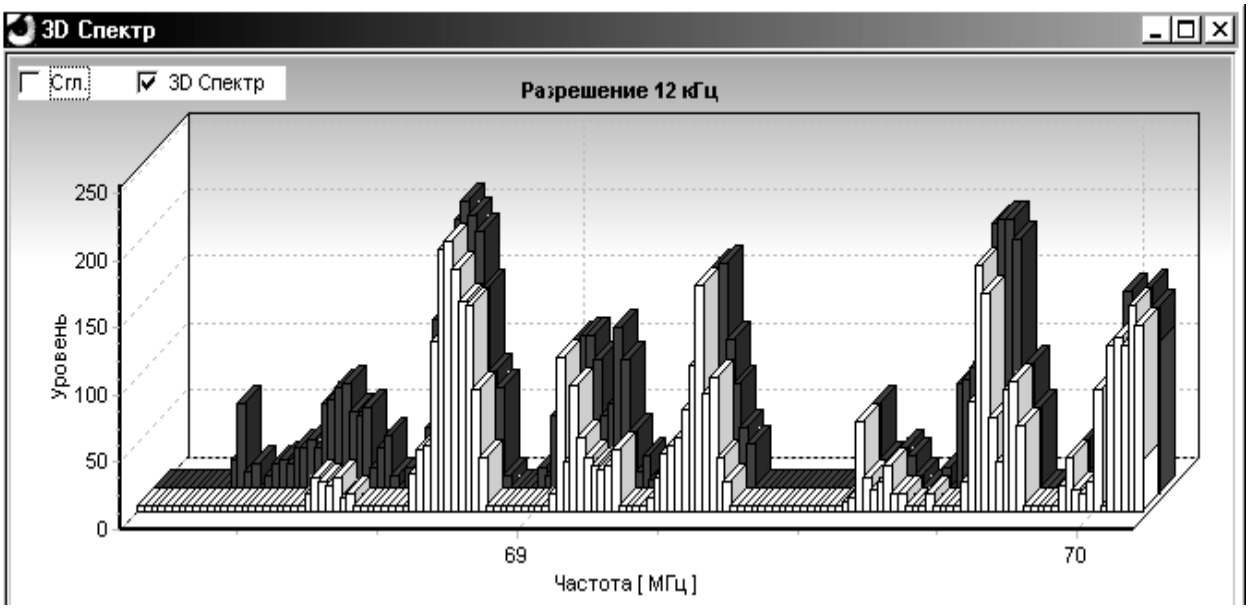


Рис. 9. Диаграмма спектра

Отмечая позиции «Сглаживание» и «3D» вид спектра можно изменять в процессе анализа. Остановить анализ можно кнопкой «Стоп». При этом картина спектра запоминается. После остановки процесса анализа можно измерять частоты и уровни спектральных составляющих, поместив курсор мыши в нужную область экрана отображения спектра. Координаты курсора, соответствующие частоте и измеренному уровню спектральной составляющей отображаются в правой части окна ниже индикатора частоты.

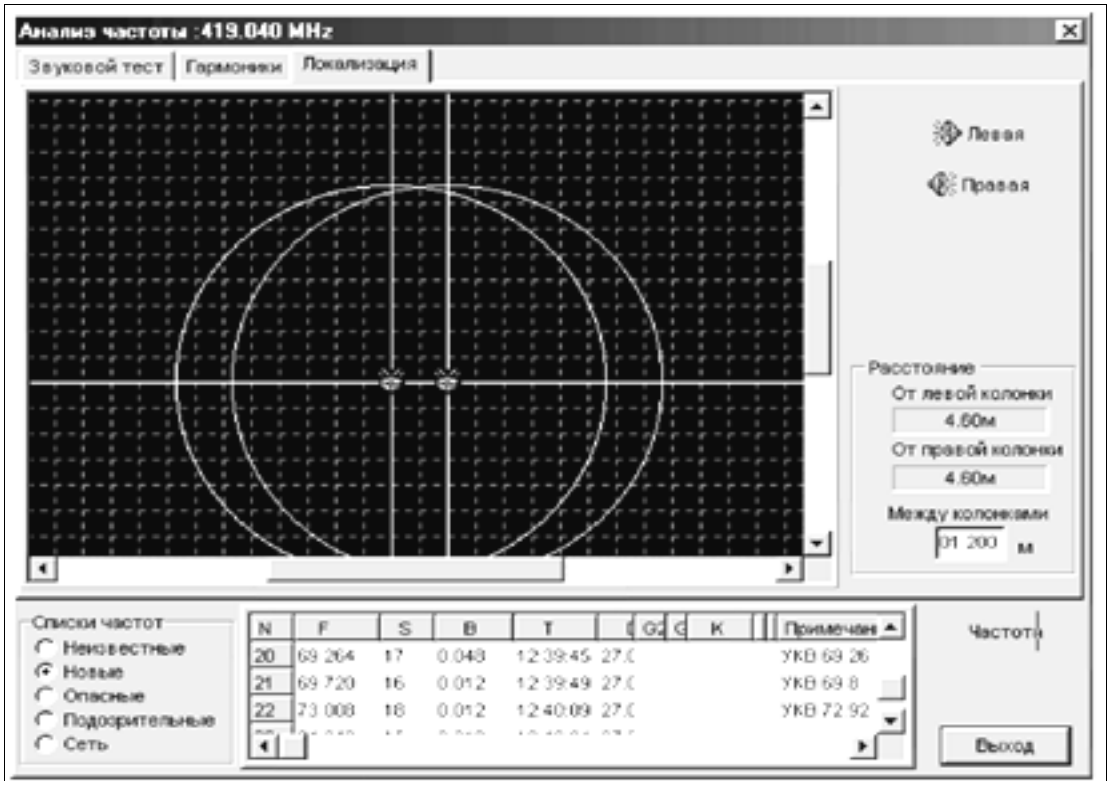


Рис. 10. Локализация радиомикрофона

Не выходя из окна спектроанализатора, можно анализировать сигналы на выходе демодулятора сканера. Подведите курсор к интересующей спектральной составляющей и щелкните левой кнопкой мыши. Сканер настроится на нужную частоту, которая отображается индикатором окна спектроанализатора. Теперь сигнал на выходе демодулятора можно прослушать или вывести на экран программы-осциллографа. Полоса пропускания сканера выбирается из выпадающего списка «Полоса анализа». Для выхода из окна анализатора спектра достаточно щелкнуть по кнопке «Выход».

5.12. Провести локализацию радиомикрофона. Для этого щелкнуть по кнопке «Анализ». В появившемся окне активизировать закладку «Локализация» и выбрать частоту обнаруженного опасного сигнала.

На экране окна появится графическая картина в виде двух пересекающихся окружностей (рис. 10). Одна из точек пересечения окружностей будет соответствовать местоположению радиомикрофона.

6. Содержание отчета

Привести задание на выполнение лабораторной работы.

Отобразить результаты экспериментальных данных, полученных при выполнении задания.

Ответить на контрольные вопросы.

7. Контрольные вопросы

7.1. Приведите определение закладочного устройства.

7.2. Перечислите демаскирующие признаки автономных некамуфлированных акустических закладок.

7.3. Перечислите демаскирующие признаки полуактивных акустических радиозакладок.

7.4. Какие технические средства применяют для выявления радиозакладочных устройств?

7.5. Назначение комплекса «RS turbo Mobile-L».

7.6. Перечислите состав комплекса «RS turbo Mobile-«L.

7.7. Радиозакладки с каким видом модуляции обнаруживает комплекс RS turbo?

7.8. Назовите базовую операцию в комплексе «RS turbo», предшествующую обнаружению и идентификации источников излучений.

7.9. Как на следующем цикле сканирования формируется новая (текущая) таблица и модифицируются значения уровней в таблице предыдущей панорамы в соответствии с выбранным методом обработки?

7.10. С помощью каких операций выполняется автоматически или в ручном режиме идентификация (опознавание) сигналов подслушивающих устройств в программе «RS turbo»?

Лабораторная работа №2

ОБНАРУЖЕНИЕ СИГНАЛОВ ЛИНЕЙНЫХ И СЕТЕВЫХ ЗАКЛАДОК

1. Цель работы

Изучить методы обнаружения сетевых и линейных закладок с помощью комплексов «RS turbo», «RS turbo Mobile-L».

2. Краткие теоретические сведения

Телефонные закладки

Линейные закладки – это встроенные в телефон устройства, предназначенные передавать беседы, проводимые в закрытой комнате при положенной на рычаг трубке, через телефонную линию. Прослушать удается как ведущиеся телефонные переговоры, так и все беседы, ведущиеся в комнате. К приемам, ориентированным на прослушивание помещения, относятся:

− прослушивание через звонковую цепь;

− внутрикомнатное прослушивание с применением высокочастотной накачки;

− встраивание «жучка», представляющего собой микрофон с электронным усилителем и активизируемого по коду через удаленный телефон;

− встраивание в аппарат «жучка», временно блокирующего рычаг трубки в ходе опускания ее после ответа на обычный телефонный звонок.

Обнаружения сетевых и линейных закладок с помощью комплексов «RS turbo», «RS turbo Mobile-L»

С помощью конвертера «RS/L plus» комплекс обнаруживает сигналы, которые передаются подслушивающими устройствами по сети электропитания или любым проводным линиям в диапазоне от 0,6 кГц до 16 МГц.

Комплекс «RS turbo Mobile-L», решает такую задачу, как обнаружение сигналов подслушивающих устройств, передающих информацию на несущих частотах по сети электропитания, телефонным или любым другим проводным линиям. Измеряет расстояние между обнаруженными передатчиками со стандартной частотной модуляцией (ЧМ) и колонками акустической системы.

При исследовании сети электропитания и проводных линий с помощью конвертора RS/L plus весь интересующий диапазон от 0,6 до 16 МГц анализируется с полосой 12,5 кГц. Эту операцию на выходе ПЧ-приемника осуществляет последовательный анализатор спектра контроллера RS turbo. Полученные данные передаются в компьютер и записываются в память.

3. Задание на выполнение работы

3.1. Изучить способы внедрения сетевых и линейных закладок.

3.2. Изучить принцип действия и порядок работы комплекса «RS turbo Mobile-L» на выявление сетевых и линейных закладок.

3.3. Выявить наличие скрытно установленного выносного микрофона с питанием от телефонной линии связи.

3.4. Выявить наличие выносного скрытно установленного микрофона с питанием от линии сети электропитания.

4. Порядок выполнения работы

4.1. Создать отдельное задание с одной или несколькими операциями сканирования сети.

4.2. В меню «Настройки» выбрать «Установка параметров». В окне «Настройка программы» щелкнуть на закладку «Задание» (рис. 1).

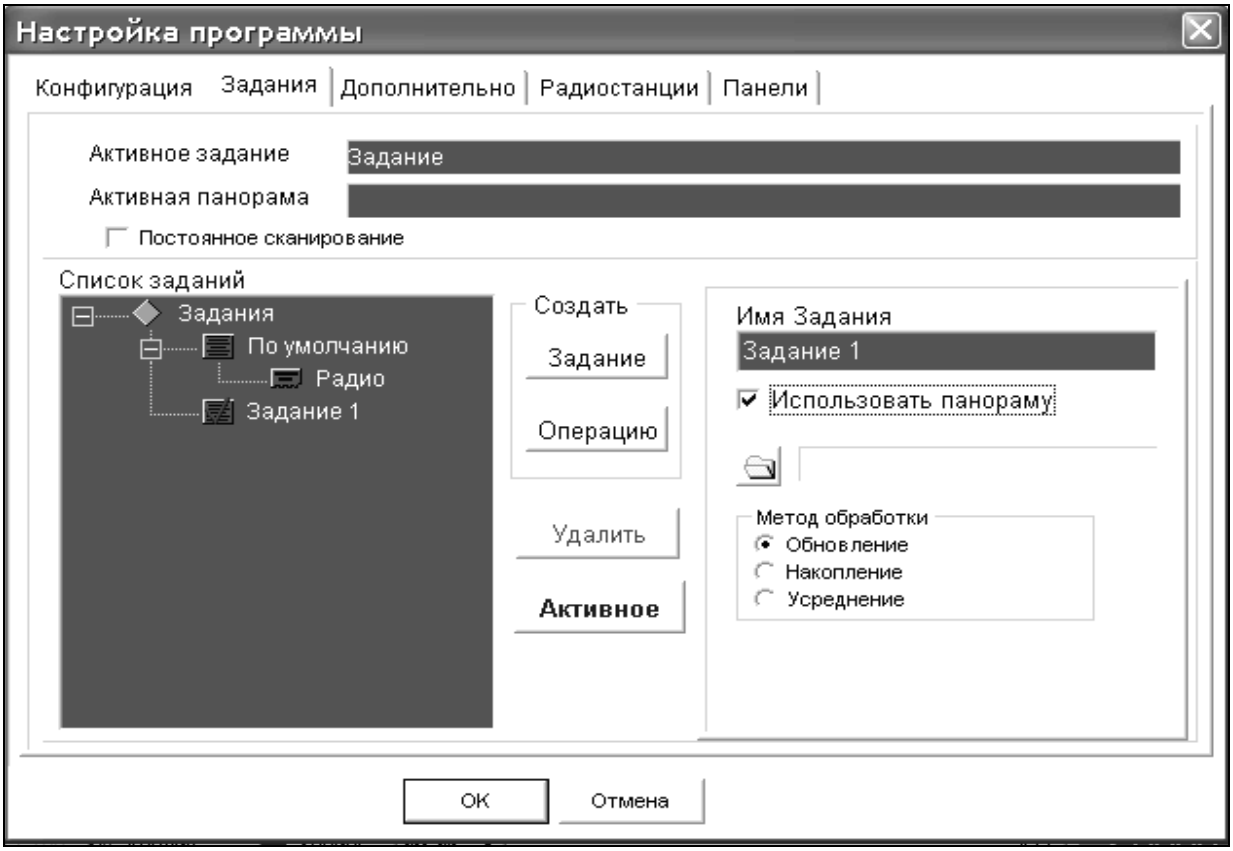


Рис. 1. Окно «Настройка программы»

4.3. Настроить параметры программы.

В закладке «Настройка программы» ввести дополнительные параметры настройки программы: принимаемый по умолчанию метод сортировки списков обнаруженных сигналов, способ оповещения о занесении в список сигнала, идентифицированного методом акустического зондирования, а также частоту преобразования конвертера RS/L. Метод сортировки определяет порядок размещения записей в списках частот обнаруженных сигналов: по возрастанию несущей частоты, максимального уровня, времени, даты обнаружения и ширине спектра обнаруженного сигнала. В данной работе выбрать метод сортировки списков обнаруженных сигналов по возрастанию несущей частоты. Выбранный в закладке метод сортировки за-

поминается и используется по умолчанию при каждом запуске программы. Его можно оперативно изменить, вызвав инструментальной кнопкой или командой «Сортировка меню – Вид – Окно – Сортировка списков» в основном окне программы. При следующем запуске программы расположение записей в списках будет соответствовать позиции, отмеченной в разделе «Сортировка списков» закладки «Дополнительно» (рис. 2).

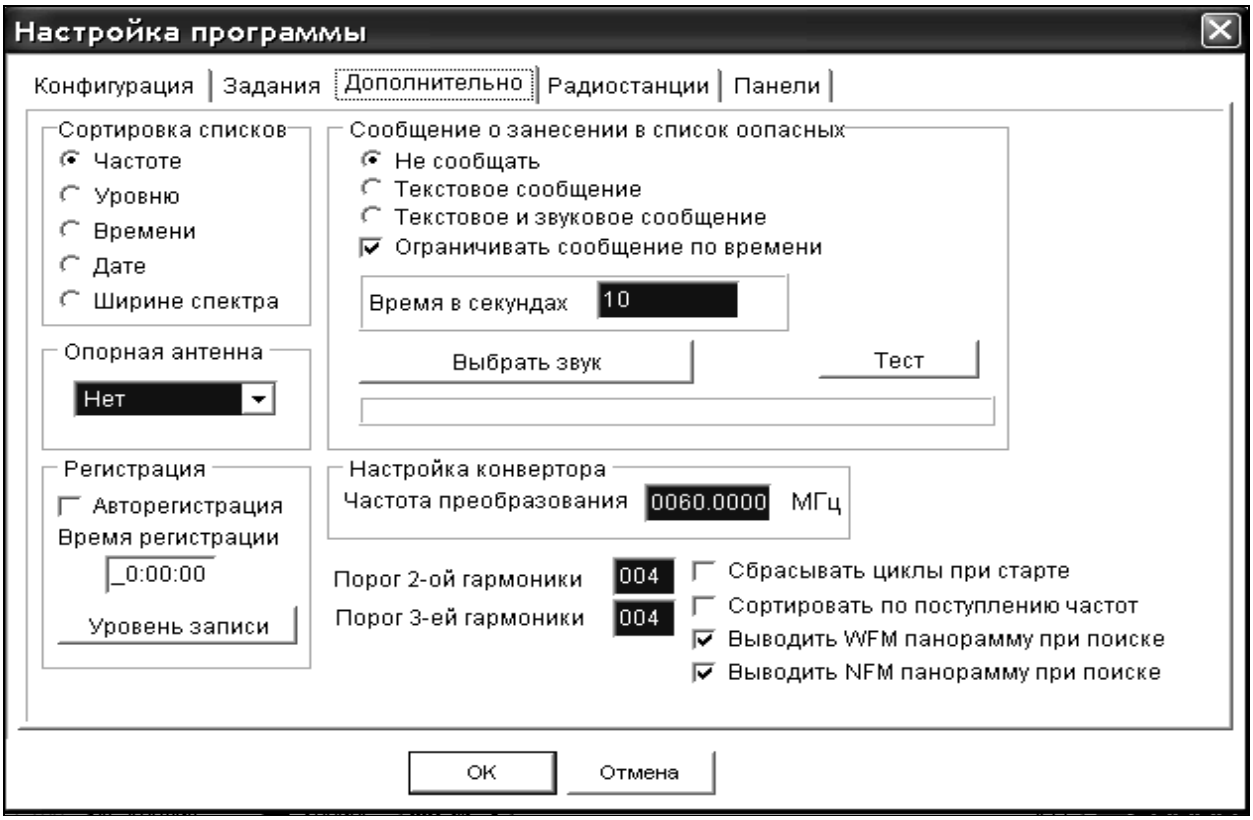


Рис. 2. Закладка «Дополнительно»

В разделе «Сообщение о занесении в список» можно выбрать метод оповещения об идентификации сигнала методом акустического зондирования или по возрастанию несущей частоты или отказаться от оповещения. Если выделить позицию «Текстовое сообщение», то при обнаружении сигнала микрофона методом акустического зондирования на экране появится сообщение: «Внимание! Обнаружен звуковой отклик! Частота 450,18 МГц». При этом процесс сканирования будет остановлен. Если отметить позицию «Ограничивать по времени и ввести время в секундах», сканирование будет возобновлено по истечении этого времени.

Отметив позицию «Текстовое и звуковое сообщение», пользователь будет дополнительно получать звуковое оповещение, которое воспроизводится через звуковую плату компьютера. Звуковое сообщение выбирается щелчком по кнопке «Выбрать звук», которая открывает стандартное окно загрузки файлов Windows. Звуковые файлы с расширением .wav из стандартного комплекта поставки Windows могут находиться в папке win-

dows\media. Имя выбранного звукового файла отображается в нижней части этого раздела закладки. Файл можно предварительно прослушать, щелкнув по кнопке «Тест». Сначала необходимо отрегулировать громкость звучания стандартной программой Windows.

В позиции ввода частоты преобразования конвертора RS/L plus необходимо записать ее значение в мегагерцах, указанное на корпусе устройства, программа сама автоматически пересчитает это значение к 12,5-кГц сетке. После завершения ввода дополнительных параметров необходимо щелкнуть по кнопке ОК. Отказаться от внесенных изменений можно щелчком по кнопке «Отмена».

4.4. Настроить частоту.

Программа RS turbo располагает возможностями быстрой настройки приемника на заданную частоту. Для настройки частоты приема сигналов в питающей сети 220 В или в проводных линиях необходимо открыть закладку «Сеть» в главном окне. Теперь цифровой индикатор отражает частоту настройки сканера относительно частоты преобразования конвертора RS/L plus, которая вводится при настройке программы и указывается слева от индикатора уровня.

Полоса обзора выбирается в закладке «Сеть» кнопками управления масштабом отображения по оси частот и может принимать только два значения: 1 и 16 МГц (значение по умолчанию – 16 МГц), причем для 1-МГц полосы отображается линейка прокрутки. Щелчок мыши в интересующей области диапазона переместит курсор и настроит сканер на ближайшую частоту из 12,5-кГц сетки. Одновременно программа включает узкую полосу пропускания сканера (нажата кнопка NFM). Для перестройки частоты на несколько 12,5 кГц-шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Кроме того, значение частоты можно ввести с клавиатуры, щелкнув левой кнопкой мыши по индикатору частоты настройки.

4.5. В окне ввода набрать частоту диапазона проводных линий (от 0,6 до 16 МГц) и щелкнуть по кнопке ОК. Введенное значение частоты программа приведет к ближайшему значению из 12,5-кГц сетки и установит частоту 16 МГц, если пользователь по ошибке укажет большее значение.

Для расширения возможностей ручного управления приемником предусмотрен быстрый просмотр частот, занесенных в списки в процессе сканирования. Если открыть соответствующий список и выделить щелчком мыши нужную запись, сканер настроится на частоту обнаруженного сигнала. Таким образом, оператор может быстро прослушать демодулированный сигнал на частотах, зафиксированных в автоматическом режиме. Последовательно настраивать приемник на частоты из списка удобно с помощью клавиш «стрелка вверх/вниз».

4.6. Измерить уровень и настройку параметров приемника.

Для измерения уровня необходимо навести на индикатор курсор мыши и нажать левую кнопку. Индикатор отражает текущее значение уровня до тех пор, пока кнопка не будет отпущена, и сохраняет это значение после отпускания кнопки мыши до выполнения очередного измерения или цикла сканирования. Тип демодулятора приемника и полоса пропускания выбирается кнопками: NFM – узкополосная частотная модуляция (ЧМ), WFM - широкополосная ЧМ, АМ – амплитудная модуляция. Справа от кнопок выбора полосы пропускания и режима демодулятора расположена кнопка управления аттенюатором АТТ. Нажатая кнопка соответствует включению дополнительного затухания, отжатая – отключению аттенюатора.

4.7. Выполнить без учета априорных данных простое сравнение составляющих измеренного с разрешением 12,5 кГц спектра сигнала с указанным в задании порогом.

4.8. Зафиксировать превышение порога. Программа запоминает частоту и уровень сигналов закладок и заносит данные в список сигналов, обнаруженных с помощью конвертора RS/L plus.

В центре главного окна размещается экран панорамного отображения спектров. Вертикальная ось экрана панорамного отображения спектров отражает интенсивность принимаемого сигнала в децибелах относительно уровня шума приемника. Горизонтальная ось соответствует частоте. Над экраном панорамы спектра находятся закладки «Радио», «Сеть» и «Панорама» (рис. 3).

Закладка «Сеть» отображает процесс и результаты сканирования диапазона поднесущих частот проводных линий от 0,6 до 16 МГц с помощью конвертера RS/L plus, а закладка «Панорама» используется для просмотра файлов спектральных панорам. Отображение спектральной панорамы в закладках «Сеть» и «Панорама» ведется с шагом 12,5 кГц. Справа находится вертикальный (столбцовый) индикатор уровня принимаемого сигнала с дополнительной цифровой индикацией и окно списков обнаруженных частот. Кнопки «Старт» и «Стоп» в нижней части экрана запускают и останавливают процесс сканирования, а кнопка «Анализ» вызывает окно для выполнения операций идентификации и классификации излучений на выделенной в списке частоте.

Рядом с кнопкой «Анализ» находятся кнопки выбора типа демодулятора сканера и управления аттенюатором, а также индикатор частоты настройки приемника с кнопками пошагового изменения частоты настройки сканера. В нижней части основного окна находятся две строки состояний. В первой отражается тип сканера, с которым работает комплекс, и время, затраченное на выполнение текущей операции сканирования. Во второй строке появляются поясняющие сообщения о функциях кнопок окна, а также имена файлов спектральной панорамы, которые используются в ка-

честве диаграммы загрузки диапазона при классификации сигналов (Активная панорама) и загружены для просмотра в закладке «Панорама» (Файл панорамы).

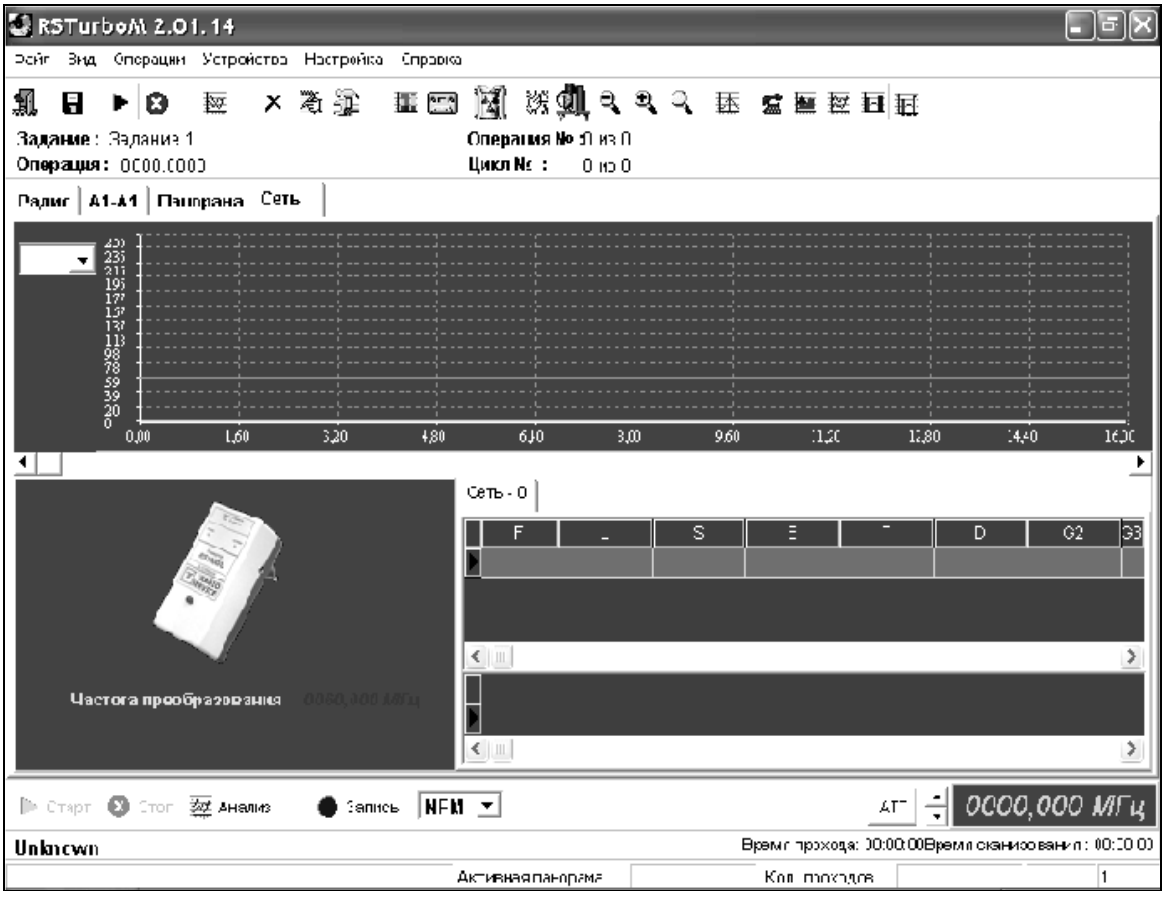


Рис. 3. Экран панорамы спектра

Для настройки частоты приема сигналов в сети 220 В или в проводных линиях необходимо открыть закладку «Сеть». В этом режиме цифровой индикатор отражает частоту настройки сканера относительно частоты преобразования конвертора RS/L plus, которая вводится при настройке программы и указывается слева от индикатора уровня. Полоса обзора выбирается в закладке «Сеть» кнопками управления масштабом отображения по оси частот и может принимать только два значения: 1 и 16 МГц (значение по умолчанию – 16 МГц), причем для 1-МГц полосы отображается линейка прокрутки. Щелчок кнопки мыши в интересующей области диапазона переместит курсор и настроит сканер на ближайшую частоту из 12,5-кГц сетки. Одновременно программа включает узкую полосу пропускания сканера (нажата кнопка NFM).

Для перестройки частоты на несколько 12,5-кГц шагов можно воспользоваться кнопками увеличить/уменьшить слева от индикатора частоты. Кроме того, значение частоты можно ввести с клавиатуры, предварительно щелкнув левой кнопкой мыши при наведенном на индикатор

частоты настройки курсоре. В окне ввода набрать частоту диапазона проводных линий (от 0,6 до 16 МГц) и щелкнуть по кнопке ОК. Введенное значение частоты программа приведет к ближайшему значению из 12,5-кГц сетки и установит частоту 16 МГц, если пользователь по ошибке укажет большее значение. Для расширения возможностей ручного управления приемником предусмотрен быстрый просмотр частот, занесенных в списки в процессе сканирования.

Если открыть соответствующий список и выделить щелчком левой кнопки мыши нужную запись, то сканер настроится на частоту обнаруженного сигнала. Таким образом, оператор может быстро прослушать демодулированный сигнал на частотах, зафиксированных в автоматическом режиме. Последовательно настраивать приемник на частоты из списка удобно с помощью клавиш стрелка вверх/вниз.

4.9. Произвести акустическое зондирование.

Кнопкой «Анализ» или командой «Анализ меню – Операции» вызвать окно анализа обнаруженных сигналов, в названии которого указывается частота анализируемого сигнала. В этом окне выбирается закладка «Звуковой тест». В верхней части закладки отображается реверберационная картина помещения, для просмотра которой можно воспользоваться линейкой прокрутки (рис. 4).

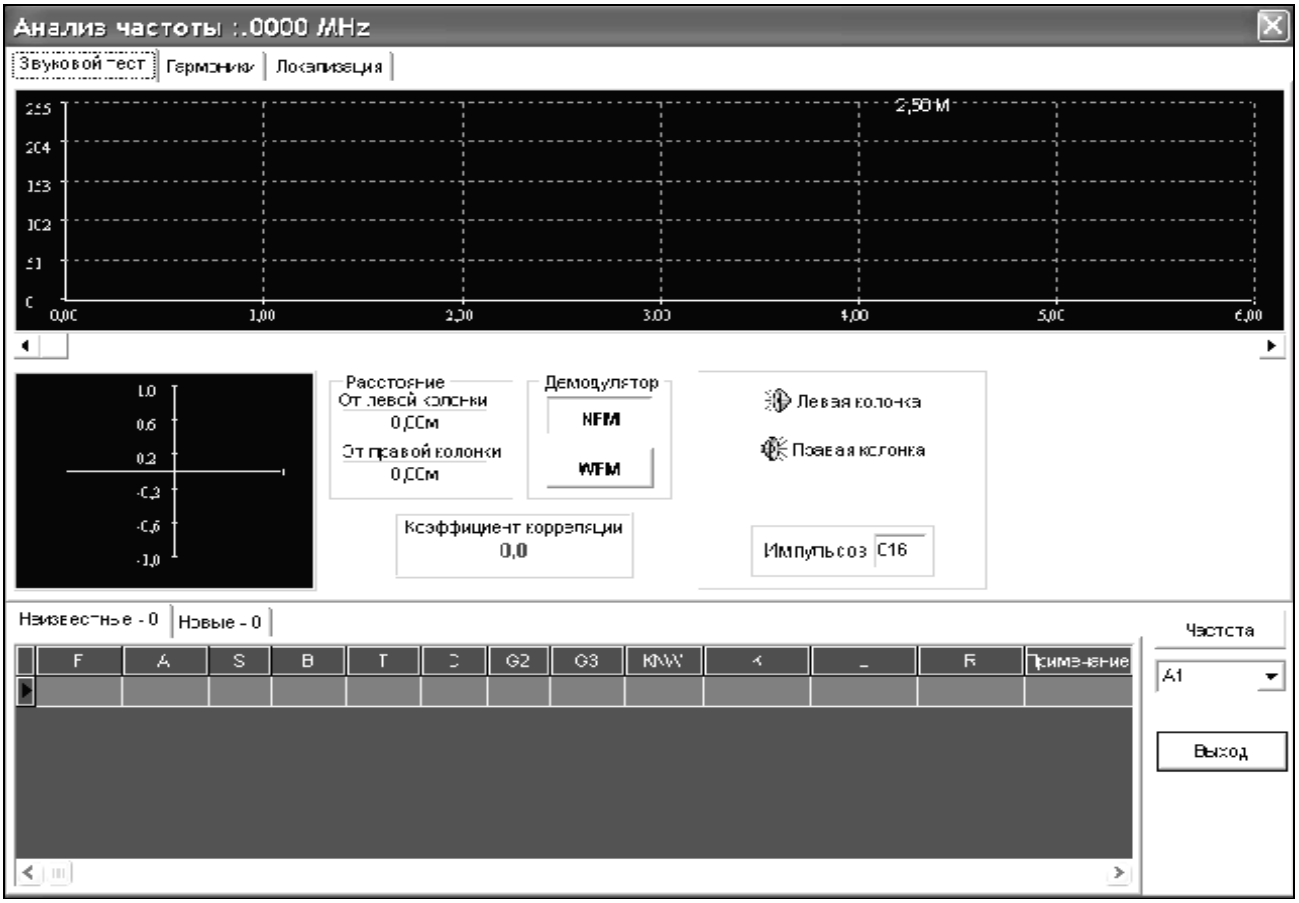


Рис. 4. Окно «Анализ частоты»

Измерить расстояние от звуковой колонки до некоторой точки, например, одного из импульсов можно, указав на него курсором мыши. При этом значение расстояния в метрах отображается в правом верхнем углу экрана реверберационной картины. В нижней части закладки отображается корреляционная функция отклика, расстояния от звуковых колонок до микрофона и значение коэффициента корреляции.

Чтобы выполнить акустический тест, необходимо из нужного списка выбрать интересующий сигнал или ввести произвольную частоту с помощью кнопки Частота, установить полосу приема (NFM или WFM), указать число циклов (импульсов) звукового зондирования и нажать кнопку с изображением левой или правой колонки. При повторном выполнении теста предыдущая реверберационная картина стирается. Закончив анализ, щелкните по кнопке Выход.

4.10. Провести анализ спектра.

Анализатор спектра вызывается инструментальной кнопкой основного окна программы или командой «Спектр – меню – Операции» (рис. 5). Полоса обзора анализатора отсчитывается вверх и вниз относительно центральной частоты. Значение полосы обзора соответствует ширине тракта ПЧ-приемника – 8 МГц. Значение центральной частоты устанавливается программой при выделении записи в одном из списков обнаруженных сигналов или вводится оператором. В последнем случае произвольно установленная центральная частота, которая может не совпадать с сеткой режима сканирования, корректируется программой.

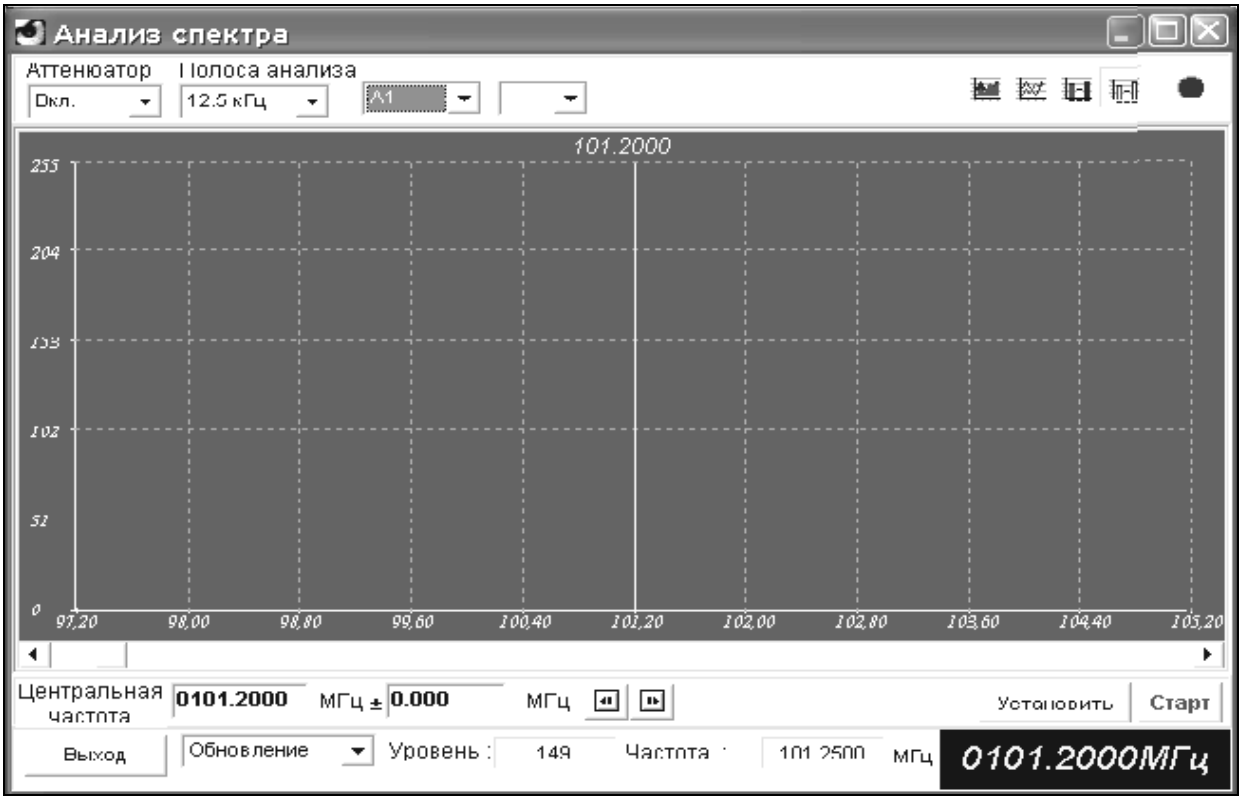


Рис. 5. Окно «Анализ спектра»

В верхней части окна находятся позиции выбора состояния аттенюатора и полосы анализа (200 или 12,5 кГц). После ввода этих параметров необходимо щелкнуть мышью по кнопке «Установить». В нижней части окна находится выпадающий список выбора режима обработки спектральных составляющих в последовательных циклах обзора.

В режиме обновления текущее значение заменяет предшествующее, в режиме накопления выбирается максимальное из этих двух значений, а в режиме усреднения – среднее. Щелчок по кнопке «Старт», включает циклический режим анализа спектра в заданной полосе обзора. Спектральные составляющие текущего цикла обзора отражаются зеленым цветом, предыдущего – красным. Отмечая позиции «Сглаживание» и «3D» вид спектра можно изменять в процессе анализа. Остановить анализ можно кнопкой «Стоп». При этом картина спектра запоминается.

После остановки процесса анализа можно измерять частоты и уровни спектральных составляющих, поместив курсор мыши в нужную область экрана отображения спектра. Координаты курсора, соответствующие частоте и измеренному уровню спектральной составляющей, отображаются в правой части окна ниже индикатора частоты.

Не выходя из окна спектроанализатора, можно анализировать сигналы на выходе демодулятора сканера. Подведите курсор к интересующей спектральной составляющей и щелкните левой кнопкой мыши. Сканер настроится на нужную частоту, которая отображается индикатором окна спектроанализатора. Теперь сигнал на выходе демодулятора можно прослушать или вывести на экран программы-осциллографа. Полоса пропускания сканера выбирается из выпадающего списка «Полоса анализа». Для выхода из окна анализатора спектра достаточно щелкнуть по кнопке «Выход».

4.11. Сохранить и просмотреть спектральную панораму.

Спектральную панораму, полученную в результате текущего и/или предшествующих циклов сканирования радиодиапазонов можно сохранить в виде файла. Для этого, после остановки сканирования, с помощью инструментальной кнопки или команды «Сохранить» меню «Файл» вызывается стандартное окно сохранения файлов Windows, где предлагается ввести имя файла и указать место его хранения. По умолчанию программа комплекса RS turbo размещает файлы спектральных панорам в папке RSturbo/Panorama. Файлы спектральных панорам должны иметь расширение .pan. Пользователь может создавать и хранить любое число таких файлов. При сохранении файла с именем, которое уже есть в папке, программа запрашивает подтверждение на перезапись.

Удалить файлы панорам можно стандартными действиями в окне Windows. Сохранение результатов сканирования диапазонов проводных линий в виде файлов не предусмотрено. Для просмотра спектральных панорам, которые сохранены в виде файлов, необходимо щелкнуть мышью по закладке «Панорама» (рис. 6).

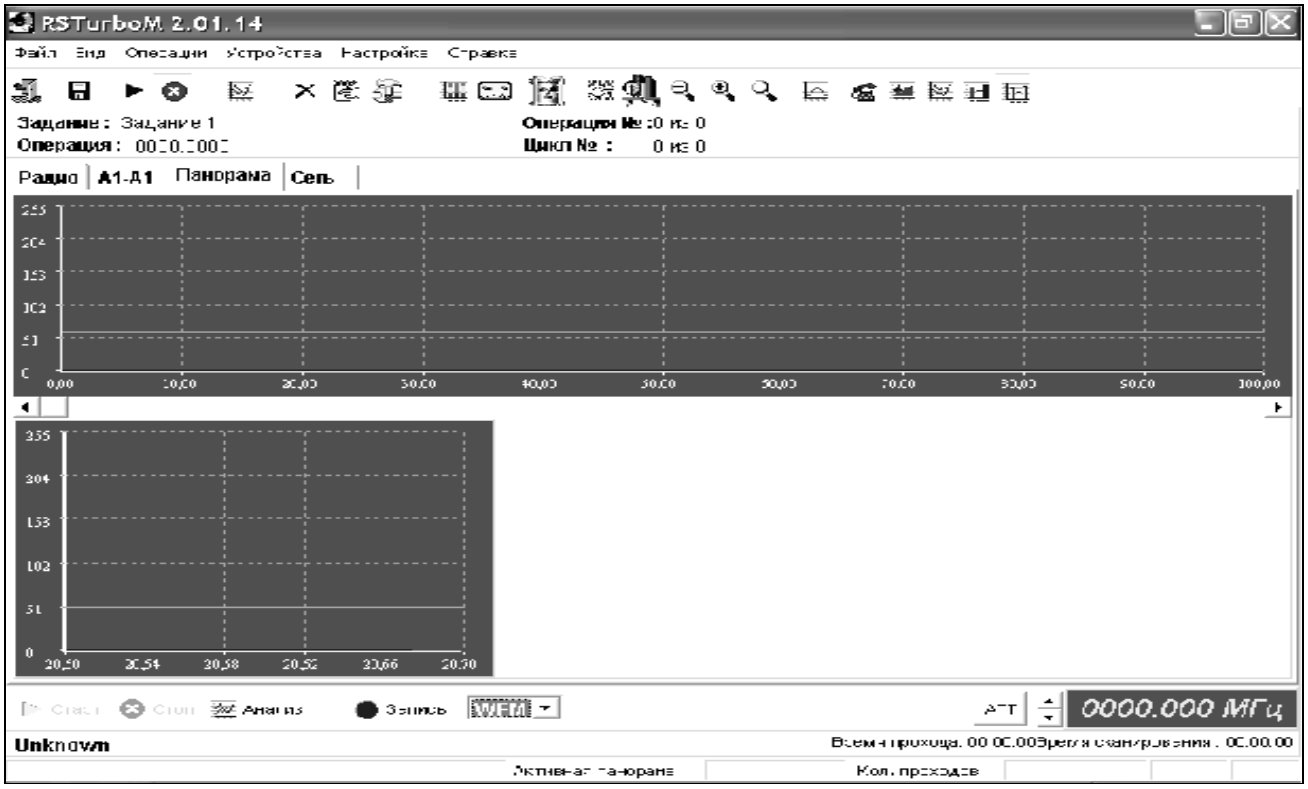


Рис. 6. Закладка «Панорама»

В режиме просмотра панорам доступна инструментальная кнопка загрузки файлов. Загрузить файл спектральной панорамы можно также командой, открыть меню «Файл», которая вызывает стандартное окно загрузки файлов Windows, где необходимо выбрать имя файла и щелкнуть по кнопке «Открыть». На экранах спектры файла панорамы отображаются синим цветом. Кнопками управления полосой обзора установите в окне спектральной панорамы удобный масштаб отображения по оси частот и найдите интересующий участок спектра с помощью линейки прокрутки и движка, которые позволяют «листать» картины спектра и быстро переходить к нужному участку диапазона. Если щелкнуть мышью на экране спектральной панорамы, в окне детального анализа будет показан спектр соответствующего участка с разрешением 12,5 кГц. Следует учитывать, что просмотр спектральной панорамы в закладке Панорама не изменяет частоты настройки сканера. Спектральная картина в закладке «Панорама» сохраняется в течение всего сеанса работы и может использоваться для сравнения с текущими спектрами, полученными в процессе сканирования.

4.12. Просмотреть список обнаруженных сигналов.

Для доступа к нужному списку обнаруженных сигналов необходимо щелкнуть левой кнопкой мыши по закладке, на которой указано название списка и текущее число записей обнаруженных сигналов в нем. Графы списков содержат следующие данные: *F* – несущая частота обнаруженного сигнала в МГц; *S* – максимальный уровень в полосе обнаруженного сигна-

ла, дБ; *B* – ширина спектра обнаруженного сигнала в МГц; *T* – время первого обнаружения сигнала, час и минуты текущих суток; *D* – дата первого обнаружения сигнала; *G*2 – уровень второй гармоники обнаруженного сигнала, дБ; *G*3 – уровень третьей гармоники обнаруженного сигнала, дБ; *K* – коэффициент корреляции при выполнении акустического теста; *L* – расстояние до микрофона от левой колонки, метры; *R* – расстояние до микрофона от правой колонки, метры. Пользователь может добавить или изменить примечание к любой записи в специальном окне, если выделить запись мышью в списке и щелкнет по ней правой кнопкой. После ввода текста примечания необходимо щелкнуть по кнопке ОК или отказаться от ввода (изменений) кнопкой «Отмена». При большом числе записей в списке появляется линейка вертикальной прокрутки. Листать списки можно также с помощью клавиш «стрелка вверх/вниз».

В программе предусмотрена возможность настройки ширины столбцов списков. Для этого необходимо навести курсор мыши на границу между столбцами в заголовке списка. После изменения формы курсора нажать левую кнопку мыши и, не отпуская ее, переместить границу столбца. Таким образом, можно настроить вид списков для отображения только тех данных, которые интересуют пользователя. Настройка ширины столбцов списка сохраняется для всех списков во всех окнах программы.

Программа комплекса «RS turbo» выполняет сортировку списков обнаруженных сигналов по различным критериям: частоте, уровню, времени, дате и ширине спектра. Для сортировки списков с помощью инструментальной кнопки или команды «Сортировка» меню – «Вид» необходимо вызвать окно сортировки, выбрать критерий сортировки и щелкнуть по кнопке ОК. Для очистки списков нажмите инструментальную кнопку «Очистить списки» или выполните команду «Очистка списков» – меню «Настройка». Появится окно (рис. 7), в котором нужно отметить те списки, все записи в которых необходимо удалить.

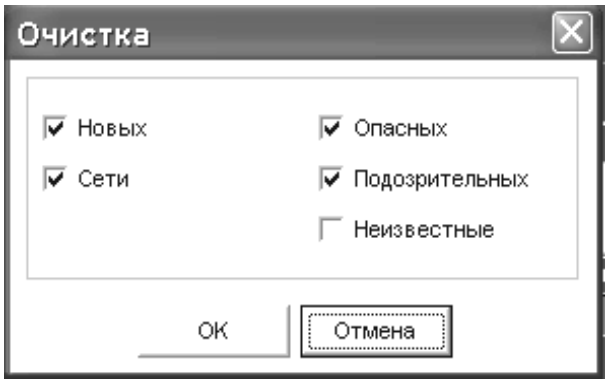


Рис. 7. Окно «Очистка»

Если отметить позицию «Неизвестные», будут удалены не только записи в списке неизвестных частот, но и данные спектральной панорамы, полученные на предыдущих циклах сканирования.

Более широкие возможности предоставляет редактор списков (рис. 8), который можно вызвать инструментальной кнопкой или командой «Редактор списков» меню «Вид». С его помощью в нужном списке можно удалить конкретную запись. Для этого необходимо открыть список, выделить мышью запись и щелкнуть по кнопке «Удалить». Если при этом пометить

позицию Удалять из панорамы спектральные компоненты этого сигнала будут удалены из текущей панорамы. Завершив работу, щелкните по кнопке ОК.

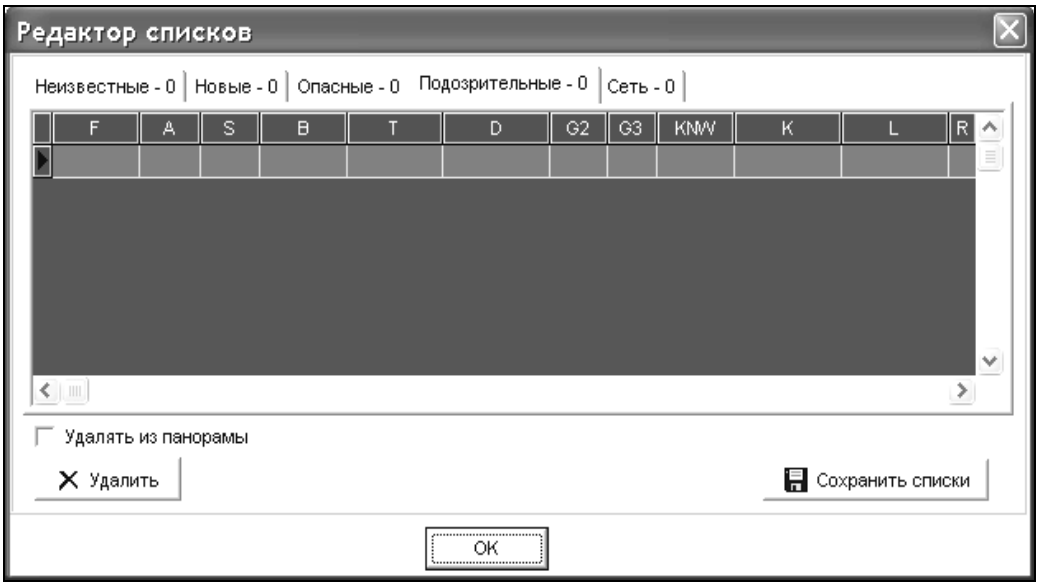


Рис. 8. Окно «Редактор списков»

5. Содержание отчета

Привести задание на выполнение лабораторной работы.

Отобразить результаты экспериментальных данных, полученных при выполнении задания. Сделать выводы по результатам работы.

Ответить на контрольные вопросы.

6. Контрольные вопросы

6.1. Назовите демаскирующие признаки сетевых акустических закладок.

6.2. Назовите демаскирующие признаки проводной микрофонной системы подслушивания.

6.3. Перечислите демаскирующие признаки акустических и телефонных закладок с передачей на высокой частоте.

6.4. Перечислите способы прослушивания беседы, ведущейся в комнате, при положенной на рычаг трубке.

6.5. По каким признакам в RS turbo возможна сортировка списков частот обнаруженных сигналов?

6.6. Поясните назначение акустического зондирования при выявлении линейной или сетевой закладки.

6.7. Результаты сканирования какого диапазона поднесущих частот проводных линий отображает закладка меню «Сеть»?

6.8. Какие действия производят в окне спектроанализатора?

6.9. Какие дополнительные параметры настройки программы вводятся в закладке «Настройка программы»?

6.10. Какие графы списков содержит окно «Редактор списков»?

Лабораторная работа №3

ОБНАРУЖЕНИЕ ОПТИЧЕСКИХ СИГНАЛОВ ПЕРЕДАТЧИКОВ ИК-ДИАПАЗОНА

1. Цель работы

Обнаружение оптических сигналов передатчиков ИК-диапазона с помощью комплексов «RS turbo», «RS turbo Mobile-L».

2. Краткие теоретические сведения

Для повышения скрытности используются для передачи перехваченной микрофоном информации инфракрасный канал. Закладки, передающие информацию по инфракрасному (ИК) каналу, более совершенны, их труднее обнаружить. Однако сложность работы с этими средствами заключается в том, что прослушать поступающую с них информацию можно только на спецприемнике, работающем в пределах прямой видимости.

В том случае, когда требуется прослушать разговоры в закрытом помещении на значительном расстоянии, используются лазерные акустические локационные системы (ЛАЛС). На практике такие системы часто называют лазерными микрофонами. ЛАЛС состоит из источника когерентного излучения (лазера) и приёмника оптического излучения, оснащённого фокусирующей оптикой. Для обеспечения высокой механической устойчивости передатчика и приёмника последние устанавливаются на треножных штативах. Передатчик и приёмник переносятся в обычном портфеле-дипломате. Как правило, в таких системах используются лазеры, работающие в ближнем ИК (0,9...1,1 мкм), невидимом глазу диапазоне длин волн.

Принцип действия системы заключается в следующем. Передатчик осуществляет облучение наружного оконного стекла узким лазерным лучом. Приёмник принимает рассеянное отраженное излучение, модулированное по амплитуде и фазе по закону изменения акустического (речевого) сигнала, возникающего при ведении разговоров в контролируемом помещении. Принятый сигнал демодулируется, усиливается и прослушивается на головных телефонах или записывается на магнитофон. Для улучшения разборчивости речи в приёмнике используется специальное шумоподавляющее устройство. Для наведения лазерного луча на цель совместно с передатчиком и приёмником используются специальные устройства – визиры.

Схема простейшего лазерного микрофона показана на рис. 1. Звуковая волна, генерируемая источником акустического сигнала, падает на границу раздела воздух-стекло со стороны помещения и создает вибрацию (отклонения поверхности стекла от исходного положения). Эти отклонения вызывают дифракцию света, отражающегося от внешней стороны стекла.

Если размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в составе различных компонент отра-

женного света будет доминировать дифракционный пучок нулевого порядка. В этом случае, во-первых, фаза световой волны оказывается промодулированной по времени с частотой звука и однородной по сечению пучка, а во-вторых, пучок «качается» с частотой звука вокруг направления зеркального отражения.

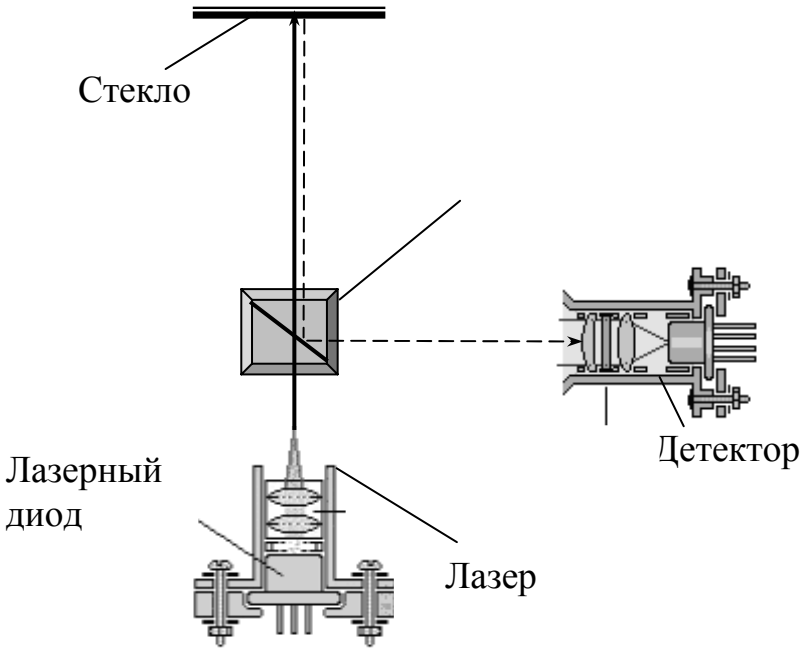


Рис. 1. Схема простейшего лазерного микрофона

Отраженное лазерное излучение принимается от сплиттера чувствительным приемником лазерного излучения (детектором). Применение сплиттера (делителя пучка) позволяет свести падающий и отражённый луч в одну точку. При демодуляции отраженного лазерного излучения выделяется речевая информация.

Лазер и приемник образуют сложную лазерную акустическую локационную систему («лазерный микрофон»), работающую в ближнем инфракрасном диапазоне волн.

Лазер, сплиттер и детектор могут быть совмещены в одном устройстве.

Данные системы наиболее эффективны для прослушивания разговоров в помещениях небольшого размера, которые по своим акустическим характеристикам близки к объёмному резонатору Гельмгольца, когда все двери и окна помещения достаточно хорошо герметизированы. Эффективны они и для подслушивания разговоров, ведущихся в салонах автомашин.

Современные ЛАЛС позволяют снимать информацию не только с наружных, но и внутренних оконных стекол, зеркал, стеклянных дверей и других предметов. В ряде случаев оконные стёкла скрытно обрабатывают специальным составом, увеличивающим коэффициент отражения лазерного излучения, а следовательно, и дальность разведки.

Лазерные акустические системы разведки имеют дальность действия при диффузном отражении до 100...300 м без специальной обработки стёкол, до 500 м – при обработке (покрытии) стёкол специальным материалом, значительно увеличивающим мощность диффузно отраженного от них лазерного излучения, и более километра – при установке на оконных стеклах специальных направленных отражателей (триппель-призм).

Средства акустической разведки могут использоваться не только для прослушивания и записи ведущихся разговоров, но и для перехвата акустических колебаний, возникающих при выводе на печать текста, например на принтер. Современные специальные комплексы обработки акустической информации позволяют восстановить текст, выводимый на печать по перехваченным акустическим излучениям.

3. Задание на выполнение работы

Сформировать список «опасных» излучений, которые могут быть созданы передатчиками.

Выполнить операции анализа, необходимые для выявления среди множества обнаруженных сигналов подслушивающих устройств.

4. Порядок выполнения работы

4.1. Создать отдельное задание

Для настройки автоматических режимов сканирования, обнаружения и идентификации в системе «RS turbo» используются задания. Задание хранится в программе и содержит все данные, используемые компьютером для управления сканирующим приемником и периферийной аппаратурой. Вместе с заданием программа сохраняет информацию, полученную при его выполнении: спектральные панорамы и списки обнаруженных сигналов. Для решения конкретных задач оператор может создавать и хранить любое число заданий. Каждое задание состоит из одной или нескольких операций двух типов проводных и оптических линий.

4.2. В меню Настройки выбрать «Установка параметров». В окне «Настройка программы» щелкнуть на закладку «Задания» (рис. 2).

4.3. Настроить дополнительные параметры программы

В этой закладке (рис. 3) вводятся некоторые дополнительные параметры настройки программы: принимаемый по умолчанию метод сортировки списков обнаруженных сигналов, способ оповещения о занесении в список сигнала, идентифицированного методом акустического зондирования, а также частота преобразования конвертера RS/L. Метод сортировки определяет порядок размещения записей в списках частот обнаруженных сигналов: по возрастанию несущей частоты, максимального уровня, времени, даты обнаружения и ширине спектра обнаруженного сигнала. Выбранный в закладке метод сортировки запоминается и используется по умолчанию при каждом запуске программы. Его можно оперативно изменить, вызвав

инструментальной кнопкой или командой «Сортировка меню – Вид – окно – Сортировка списков» в основном окне программы.

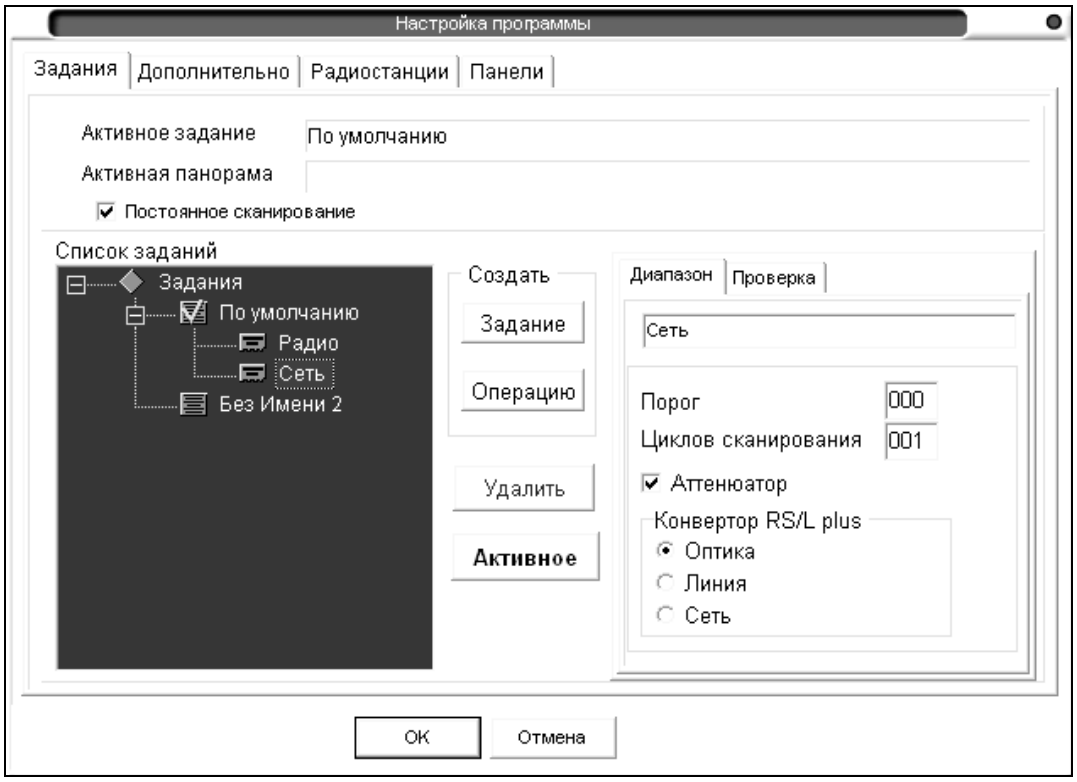


Рис. 2. Закладка «Задания»

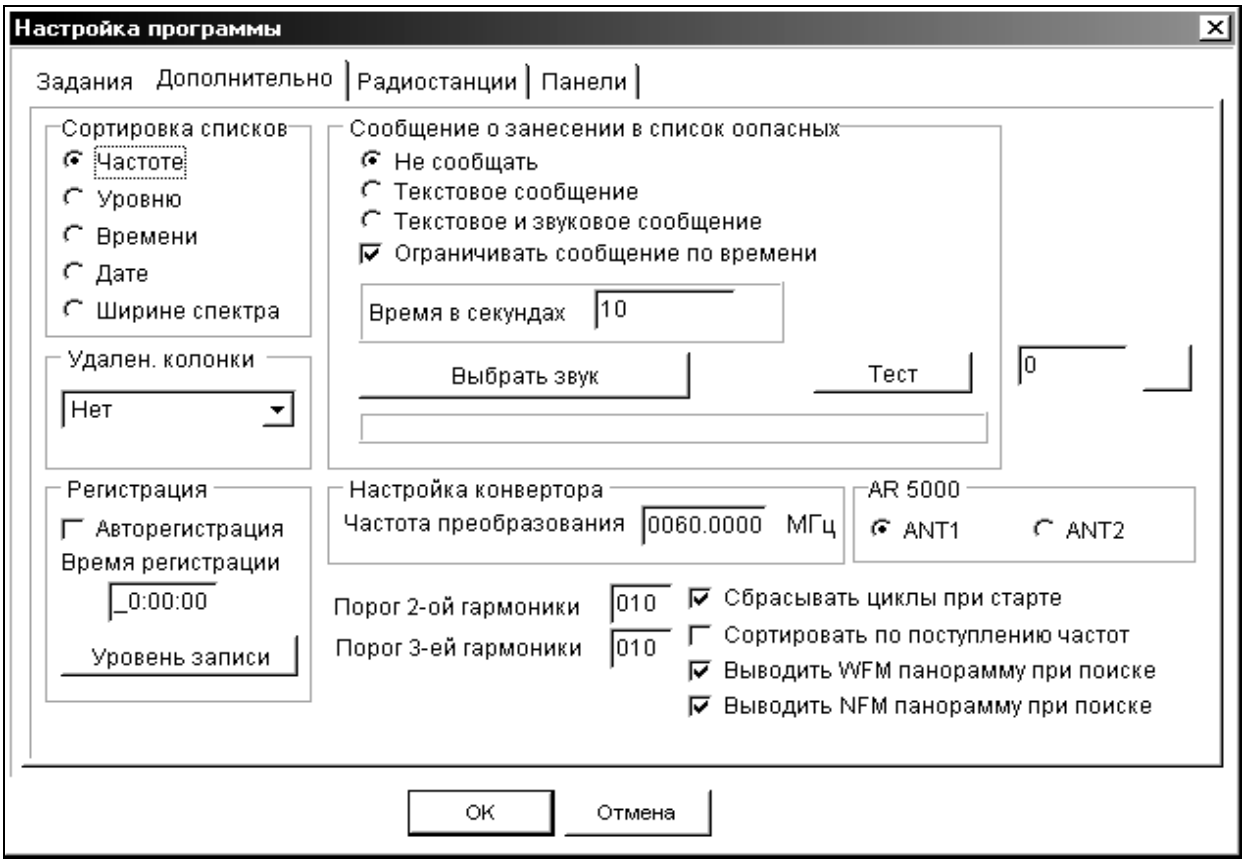


Рис. 3. Закладка «Дополнительно»

При следующем запуске программы расположение записей в списках будет соответствовать позиции, отмеченной в разделе «Сортировка списков» закладки «Дополнительно».

В разделе «Сообщение о занесении в список» можно выбрать метод оповещения об идентификации сигнала методом акустического зондирования или отказаться от оповещения. Если выделить позицию «Текстовое сообщение», то при обнаружении сигнала радиомикрофона методом акустического зондирования на экране появится сообщение: «Внимание! Обнаружен звуковой отклик! Частота 450,18 МГц». При этом процесс сканирования будет остановлен.

Если отметить позицию «Ограничивать по времени» и ввести время в секундах, сканирование будет возобновлено по истечении этого времени. Отметив позицию «Текстовое и звуковое сообщение», пользователь будет дополнительно получать звуковое оповещение, которое воспроизводится через звуковую плату компьютера. Звуковое сообщение выбирается щелчком по кнопке «Выбрать звук», которая открывает стандартное окно загрузки файлов Windows.

Звуковые файлы с расширением .wav из стандартного комплекта поставки Windows могут находиться в папке windows\media. Имя выбранного звукового файла отображается в нижней части этого раздела закладки. Файл можно предварительно прослушать, щелкнув по кнопке Тест. Прежде необходимо отрегулировать громкость звучания стандартной программой Windows. В позиции ввода частоты преобразования конвертора «RS/L plus» необходимо записать ее значение в МГц, указанное на корпусе устройства, программа сама автоматически пересчитает это значение к 12,5-кГц сетке. После завершения ввода дополнительных параметров необходимо щелкнуть по кнопке OK. Отказаться от внесенных изменений можно щелчком по кнопке «Отмена».

4.4. Провести сканирование и обнаружение

Для запуска операций сканирования необходимо активизировать требуемое задание в окне «Настройка программы», выбрать нужную закладку экрана спектральной панорамы «Сеть» и щелкнуть по инструментальной кнопке или кнопке «Старт» внизу основного окна программы. После активизации задания в основное окно программы будет загружена спектральная панорама (красного цвета) и списки обнаруженных сигналов, созданные в ходе предыдущих сеансов работы по данному заданию с момента последней очистки панорамы и/или списков (при первой активизации задания панорамы списки будут пусты). Если в задании предусмотрено использование диаграммы загрузки, ее спектральная панорама будет выведена на задний план синим цветом. После запуска сканирования программа начинает построение текущей спектральной панорамы, которая отображается на переднем плане зеленым цветом. В процессе сканирования можно вы-

бирать удобный масштаб отображения спектральной панорамы по оси частот. Обнаружив сигнал, программа заносит его параметры в списки в соответствии с выбранными критериями классификации и выполняет тесты идентификации, если они предусмотрены в задании. Просмотреть списки в процессе сканирования можно, щелкая по нужной закладке и выбирая запись с помощью линейки вертикальной прокрутки. Если сигнал был обнаружен и занесен в список (списки) в ходе предыдущих сеансов работы или циклов сканирования, то при повторном обнаружении он в списки не заносится. Чтобы в процессе сканирования фиксировать все обнаруженные сигналы, необходимо предварительно очистить список «неизвестных» излучений. После выполнения всех операций задания программа останавливается и переходит к основному окну. Остановить сканирование можно кнопкой «Стоп».

4.5. Провести акустическое зондирование

Кнопкой с надписью «Анализ» или командой «Анализ – меню – Операции» вызывается окно анализа обнаруженных сигналов, в названии которого указывается частота анализируемого сигнала. В этом окне выбирается закладка «Звуковой тест». В верхней части закладки отображается реверберационная картина помещения, для просмотра которой можно воспользоваться линейкой прокрутки (рис. 4).

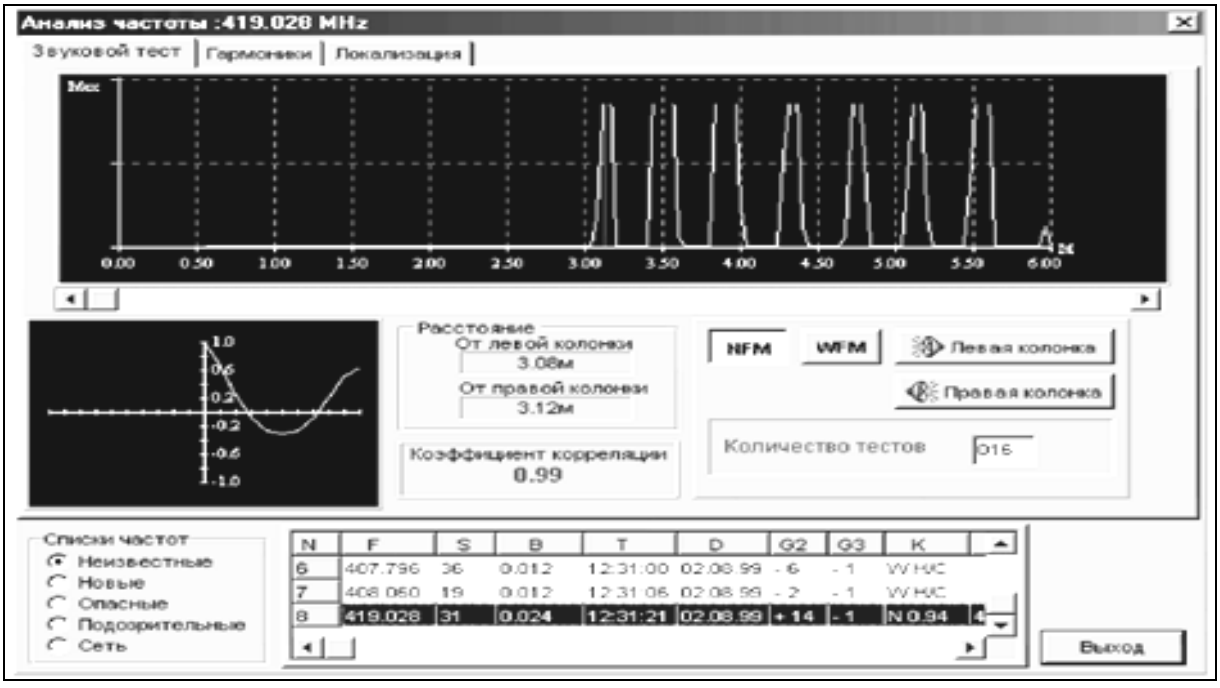


Рис. 4. Окно звукового зондирования

Измерить расстояние от звуковой колонки до некоторой точки, например, одного из импульсов можно, указав на него курсором мыши. При этом значение расстояния в метрах отображается в правом верхнем углу экрана реверберационной картины. В нижней части закладки отображается корре-

ляционная функция отклика, расстояния от звуковых колонок до микрофона и значение коэффициента корреляции. Чтобы выполнить акустический тест, необходимо из нужного списка выбрать интересующий сигнал или ввести произвольную частоту с помощью кнопки «Частота», установить полосу приема (NFM или WFM), указать число циклов (импульсов) звукового зондирования и нажать кнопку с изображением левой или правой колонки. При повторном выполнении теста предыдущая реверберационная картина стирается.

Закончив анализ, щелкните по кнопке «Выход».

4.6. Провести анализ спектра

Анализатор спектра вызывается инструментальной кнопкой основного окна программы или командой «Спектр – меню – Операции». Полоса обзора анализатора отсчитывается вверх и вниз относительно центральной частоты. Значение полосы обзора соответствует ширине тракта ПЧ-приемника – 8 МГц. Значение центральной частоты устанавливается программой при выделении записи в одном из списков обнаруженных сигналов или вводится оператором. В последнем случае произвольно установленная центральная частота, которая может не совпадать с сеткой режима сканирования, корректируется программой.

В верхней части окна находятся позиции выбора состояния аттенюатора и полосы анализа (12,5 кГц или 200 кГц). После ввода этих параметров необходимо щелкнуть левой кнопкой мыши по инструментальной кнопке «Установить». В нижней части окна находится выпадающий список выбора режима обработки спектральных составляющих в последовательных циклах обзора. В режиме обновления текущее значение заменяет предшествующее, в режиме накопления выбирается максимальное из этих двух значений, а в режиме усреднения – среднее. Щелчок по кнопке «Старт» включает циклический режим анализа спектра в заданной полосе обзора. Спектральные составляющие текущего цикла обзора отражаются зеленым цветом, предыдущего – красным. Отмечая позиции «Сглаживание и 3D» вид спектра можно изменять в процессе анализа. Остановить анализ можно кнопкой «Стоп». При этом картина спектра запоминается. После остановки процесса анализа можно измерять частоты и уровни спектральных составляющих, поместив курсор мыши в нужную область экрана отображения спектра. Координаты курсора, соответствующие частоте и измеренному уровню спектральной составляющей отображаются в правой части окна ниже индикатора частоты. Не выходя из окна спектроанализатора, можно анализировать сигналы на выходе демодулятора сканера. Подведите курсор к интересующей спектральной составляющей и щелкните левой кнопкой мыши. Сканер настроится на нужную частоту, которая отображается индикатором окна спектроанализатора. Теперь сигнал на выходе демодулятора можно прослушать или вывести на экран программы-осциллографа.

Полоса пропускания сканера выбирается из выпадающего списка «Полоса анализа». Для выхода из окна анализатора спектра достаточно щелкнуть по кнопке «Выход».

4.7. Провести сохранение и просмотр спектральных панорам

Для этого после остановки сканирования с помощью инструментальной кнопки или команды «Сохранить меню – Файл» вызывается стандартное окно сохранения файлов Windows, где предлагается ввести имя файла и указать место его хранения. По умолчанию программа комплекса «RS turbo» размещает файлы спектральных панорам в папке RSturbo/Panorama. Файлы спектральных панорам должны иметь расширение .pan. Пользователь может создавать и хранить любое число таких файлов. При сохранении файла с именем, которое уже есть в папке, программа запрашивает подтверждение на перезапись. Удалить файлы панорам можно стандартными действиями в окне Windows. Сохранение результатов сканирования диапазонов проводных линий в виде файлов не предусмотрено. Для просмотра спектральных панорам, которые сохранены в виде файлов, необходимо щелкнуть мышью по закладке «Панорама». В режиме просмотра панорам доступна инструментальная кнопка загрузки файлов. Загрузить файл спектральной панорамы можно также командой «Открыть меню – Файл», которая вызывает стандартное окно загрузки файлов Windows, где необходимо выбрать имя файла и щелкнуть по кнопке «Открыть». На экранах спектры файла панорамы отображаются, синим цветом. Кнопками управления полосой обзора установите в окне спектральной панорамы удобный масштаб отображения по оси частот и найдите интересующий участок спектра с помощью линейки прокрутки и бегунка, которые позволяют «листать» картины спектра и быстро переходить к нужному участку диапазона. Если щелкнуть мышью на экране спектральной панорамы, в окне детального анализа будет показан спектр соответствующего участка с разрешением 12,5 кГц. Следует учитывать, что просмотр спектральной панорамы в закладке Панорама не изменяет частоты настройки сканера. Спектральная картина в закладке «Панорама» сохраняется в течение всего сеанса работы и может использоваться для сравнения с текущими спектрами, полученными в процессе сканирования.

4.8. Проанализировать списки обнаруженных сигналов

Для доступа к нужному списку обнаруженных сигналов необходимо щелкнуть мышью по закладке, на которой указано название списка и текущее число записей (обнаруженных сигналов) в нем. Графы списков содержат следующие данные: *F* – несущая частота обнаруженного сигнала, МГц; S – максимальный уровень в полосе обнаруженного сигнала, дБ; *B* – ширина спектра обнаруженного сигнала, МГц; *T* – время первого обнаружения сигнала, час и минуты текущих суток; *D* – дата первого обнаружения сигнала; *G*2 – уровень второй гармоники обнаруженного сигнала, дБ; *G*3 –

уровень третьей гармоники обнаруженного сигнала, дБ; *K* – коэффициент корреляции при выполнении акустического теста; *L* – расстояние до микрофона от левой колонки в метрах; *R* – расстояние до микрофона от правой колонки в метрах. В графу примечания программа помещает имя внешней радиостанции, если обнаруженный сигнал попал в полосу занимаемых ее частот. Кроме того, пользователь может добавить или изменить примечание к любой записи в специальном окне, если выделить запись в списке и щелкнуть по ней правой кнопкой мыши. После ввода текста примечания необходимо щелкнуть по кнопке OK или отказаться от ввода (изменений) кнопкой «Отмена». При большом числе записей в списке появляется линейка вертикальной прокрутки. Листать списки можно также с помощью клавиш стрелка вверх/вниз.

В программе предусмотрена возможность настройки ширины столбцов списков. Для этого необходимо навести курсор мыши на границу между столбцами в заголовке списка. После изменения формы курсора нажать левую кнопку мыши и, не отпуская ее, переместить границу столбца. Таким образом, можно настроить вид списков для отображения только тех данных, которые интересуют пользователя. Настройка ширины столбцов списка сохраняется для всех списков во всех окнах программы. Программа комплекса RS turbo выполняет сортировку списков обнаруженных сигналов по различным критериям: частоте, уровню, времени, дате и ширине спектра. Для сортировки списков с помощью инструментальной кнопки или команды «Сортировка – меню – Вид» необходимо вызвать окно сортировки, выбрать критерий сортировки и щелкнуть по кнопке OK.

Для очистки списков нажмите инструментальную кнопку «Очистить списки» или выполните команду «Очистка списков – меню – Настройка». Появится окно (рис. 5), в котором нужно отметить те списки, все записи в которых необходимо удалить. Если отметить позицию «Неизвестные», будут удалены не только записи в списке неизвестных частот, но и данные спектральной панорамы, полученные на предыдущих циклах сканирования.

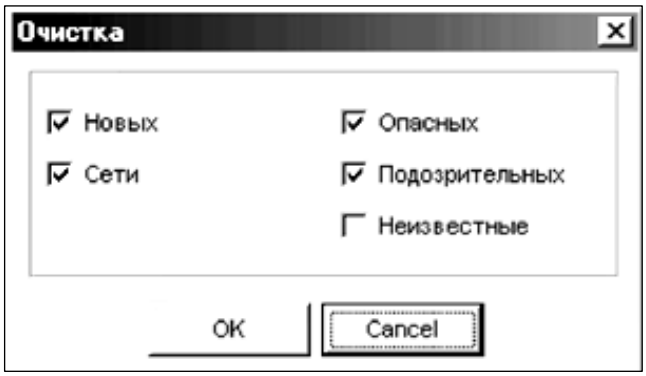


Рис. 5. Окно очистки списков

Более широкие возможности предоставляет редактор списков (рис. 6), который можно вызвать инструментальной кнопкой или командой «Редактор списков меню – Вид». С его помощью в нужном списке можно удалить конкретную запись. Для этого необходимо открыть список, выделить курсором мыши запись и щелкнуть по кнопке «Удалить». Если при этом пометить позицию «Удалить из панорамы», спектральные компонен-

ты этого сигнала будут удалены из текущей панорамы. Завершив работу, щелкните по кнопке OK.

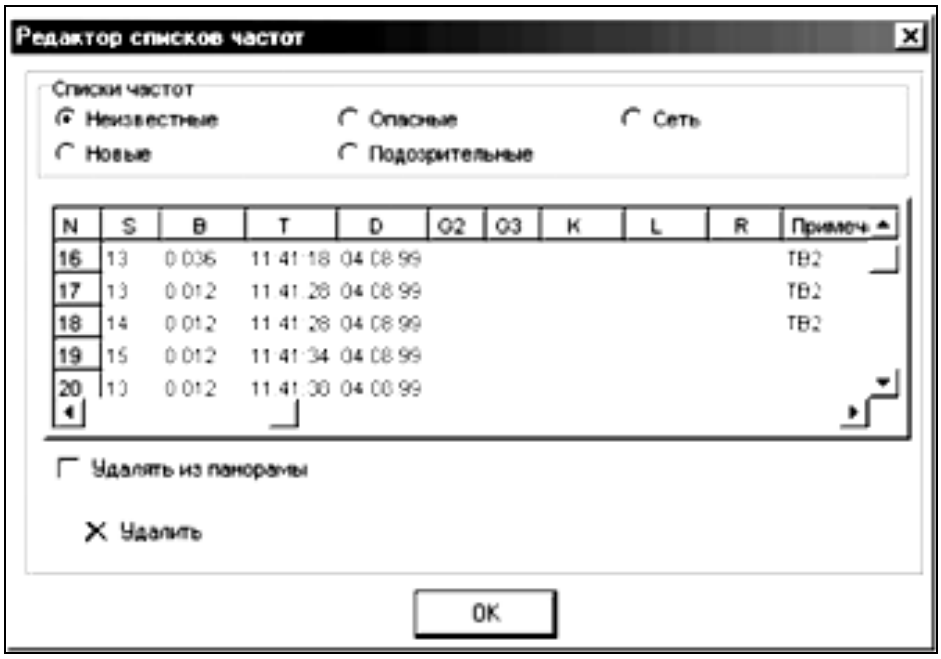


Рис. 6. Окно редактора списков частот

5. Содержание отчета

Привести задание на выполнение лабораторной работы. Отобразить результаты экспериментальных данных, полученных при выполнении задания. Ответить на контрольные вопросы.

6. Контрольные вопросы

6.1. Укажите на основные особенности канала для сигналов ИК-диапазона.

6.2. Каким образом передается речевой сигнал с помощью ИК-излучения?

6.3. Перечислите способы защиты от утечки речевой информации по ИК-каналу.

Лабораторная работа №4

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «СПРУТ-7»

1. Цель работы

Изучить назначение комплекса Спрут-7, его состав и возможности. Изучить возможности управления комплексом при помощи специального программного обеспечения.

2. Краткие теоретические сведения

Звуковые волны в газообразных и жидких средах являются продольными (т.е. такими, в которых направления смещения частиц среды совпадают с направлением распространения волны); в твердых средах кроме продольных могут иметь место поперечные волны и их комбинации (изгибные, крутильные и т.п.).

Важнейшими характеристиками звуковых волн являются следующие:

- Диапазон частот, воспринимаемых человеческим ухом (Гц) – 16 Гц ... 20 кГц (< 16 Гц – инфразвук, > 20 кГц – ультразвук).
- Скорость распространения звуковых волн в среде (скорость звука), V (м/с); при неизменных условиях распространения (температура, атмосферное давление и т.п.), V = const. Скорость звука в воздухе равна 331 м/с (при $t° - 0$ °С, $P = 1$ атм), в воде – 1490 м/с (20 °С), в бетоне 4200 ... 5300 м/с.
- Длина волны $\lambda = V/f$, где f – частота звука в Гц. Для звуковых волн λ = 1,65 см...20,7 м.

С точки зрения физики речевой сигнал представляет собой сложный частотно- и амплитудно-модулированный колебательный процесс. Частотный диапазон речи лежит в пределах 70…7000 Гц. Усредненный спектр русской речи приведен на рис. 1.

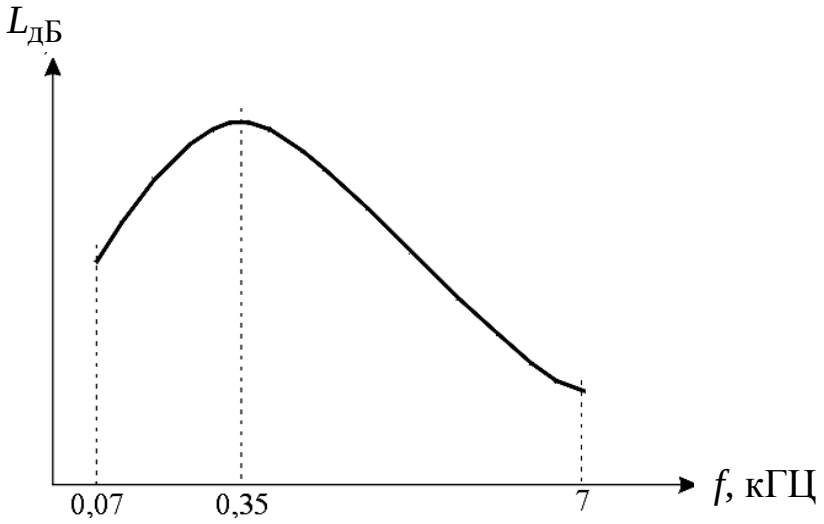


Рис. 1. Усредненный спектр русской речи

При распространении звуковая волна оказывает давление на среду, в которой она распространяется. Это давление называется звуковым. Строго говоря, это переменная часть давления, т.е. разность между мгновенными значениями давления в точке среды при прохождении волны и статическим давлением в этой же точке. Давление представляет собой силу, действующую на единицу поверхности: $P = F/S$. Единицей измерения давления в системе СИ является Паскаль (Па), Ньютон/ м^2.

Звуковое давление в воздухе изменяется от $P_0 = 2 \cdot 10^{-5}$ Па (порог слышимости) до 10^5 Па (болевой порог).

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

$$L_{\text{дБ}} = 20\lg\frac{P}{P_0}.$$

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

Принятые центральные частоты стандартных октавных полос соответствуют следующему ряду: 2, 4, 8, 16, 31.5, 63, 125, 250, 500 (Гц), 1, 2, 4, 8, 16 (кГц).

Соотношение между центральной полосой i-й октавы и ее граничными частотами следующее:

$$f_{\text{верх}} = f_{\text{центр},i} \cdot \sqrt{2};$$

$$f_{\text{нижн}} = \frac{f_{\text{центр},i}}{\sqrt{2}}.$$

Для оценки параметров речи в связи со сложностью расчетов и с учетом частотного диапазона речи, принято использовать 5 октавных полос с центральными частотами 250, 500, 1000, 2000, 4000 (Гц).

3. Описание комплекса «Спрут-7»

Программно-аппаратный комплекс «Спрут-7» предназначен для проверки выполнения норм эффективности защиты речевой информации от её утечки по акустическому и виброакустическому каналам, а также за счет прямых низкочастотных акустоэлектрических преобразований.

Комплекс обеспечивает измерение характеристик акустических сигналов, в том числе октавный, треть октавный анализ и анализ с использованием функции быстрого преобразования Фурье (БПФ); проведение исследований характеристик и проверку эффективности систем акустического и виброакустического зашумления; измерение уровней сигналов акустоэлектрических преобразователей с использованием функции БПФ.

Комплекс может использоваться также при измерении и гигиенической оценке шумов и вибрации в жилых и производственных помещениях на соответствие санитарным нормам.

3.1. Технические характеристики и возможности комплекса

Технические характеристики комплекса, представлены в табл. 3.1.

Таблица 3.1

Технические характеристики комплекса «Спрут-7»

Технические характеристики	Значение технических характеристик
1. Частотный диапазон, Гц	1–20000
2. Диапазон частот фильтров, Гц: 1/1-октавные фильтры по ГОСТ 17168 1/3-октавные фильтры по ГОСТ 17168	 2–16000 2–20000
3. Диапазон измеряемых уровней звукового давления, дБ	24–130
4. Диапазон измерения общего виброускорения, $м \cdot с^{-2}$	0,01–708
5. Предел основной погрешности измерений: уровня звукового давления, дБ уровня виброускорения, дБ	 ±0,7 ±0,7
6. Пороговая чувствительность входного напряжения, нВ	100
7. Коэффициент усиления адаптеров-усилителей, дБ	20, 40 и 40, 60
8. Время работы от аккумуляторов, не менее, час.	7
9. Масса, кг	25

3.2. Состав комплекса Спрут-7

Программно-аппаратный комплекс «Спрут-7» состоит из трех подсистем:

– измерительной подсистемы;

– подсистемы источника тестового акустического сигнала;

– подсистемы управления.

3.2.1. Измерительная подсистема

Основной задачей измерительной подсистемы является получение измеряемой информации с внешнего датчика, ее обработка и пересылка в подсистему управления.

Измерительная подсистема создана на базе анализатора шума и вибраций 1-го класса точности SVAN-947 и состоит:

– из измерительного модуля;

– из измерительного микрофона – для акустических измерений;

– из измерительного вибродатчика – для виброакустических измерений;

– из дифференциальных усилителей (20 дБ, 40 дБ) – для измерений сигналов, образующихся за счет акустоэлектрических преобразований;

– измерительной антенны EMCO 6511;

– стойки для установки измерительного модуля;

– антенны для сопряжения с подсистемой управления по радиоканалу.

Измерительный модуль

Измерительный модуль обеспечивает:

– формирование питающих напряжений и токов, необходимых для нормального функционирования подключаемых датчиков;

– усиление маломощных электрических сигналов от датчиков;

– аналогово-цифровое преобразование и измерение;

– предварительную цифровую обработку результатов измерений (фильтрация, расчет интегрального уровня сигнала, октавный анализ, третьоктавный анализ, функция быстрого преобразования Фурье (БПФ));

– отображение результатов измерений на встроенном жидкокристаллическом индикаторе;

– передачу результатов измерений в управляющую ПЭВМ, через модуль сопряжения по радиоканалу в цифровом виде;

– проверку значений напряжения встроенного источника электропитания, индикацию состояния электропитания.

Вход измерительного модуля выполнен с применением разъема типа BNC. Корпус разъема соединен с корпусом прибора. На центральный контакт подается измеряемый сигнал от датчиков.

На центральном контакте разъема измерительного входа присутствует постоянное напряжение 28 В.

Не допускается подключение к входу измерительного модуля любых нештатных устройств и подача непосредственно на вход измерительного модуля любых сигналов. Это может привести к выходу из строя измерительного модуля.

Используемые в измерительном модуле разъемы гарантируют надежный электрический контакт. Данные разъемы очень чувствительны к механическим воздействиям, поэтому нельзя применять силу при соединении/разъединении разъемов.

Внешний вид измерительного модуля приведен на рис. 2.

Рис. 2. Внешний вид измерительного модуля

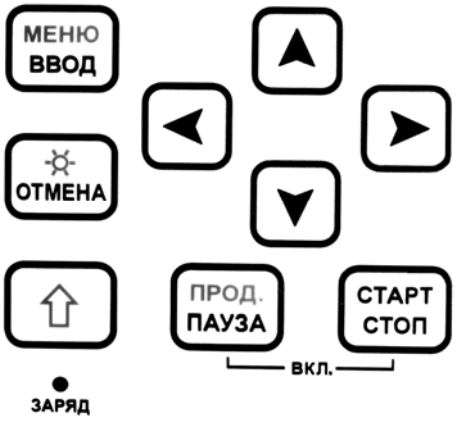


Рис. 3. Управляющие клавиши измерительного модуля

На передней панели прибора находятся девять управляющих клавиш (рис. 3).

Включение и выключение прибора осуществляется путем одновременного нажатия, а затем отпускания клавиш ПРОД. ПАУЗА и СТАРТ СТОП

При использовании в составе комплекса «Спрут-7» управление измерительным модулем осуществляется программно, без участия оператора. Все что нужно сделать – это включить прибор.

Измерительный микрофон

Измерительный микрофон является датчиком, предназначенным для измерения уровней акустических сигналов. Он подключается непосредственно к измерительному модулю.

Внешний вид измерительного микрофона приведен на рис. 4.

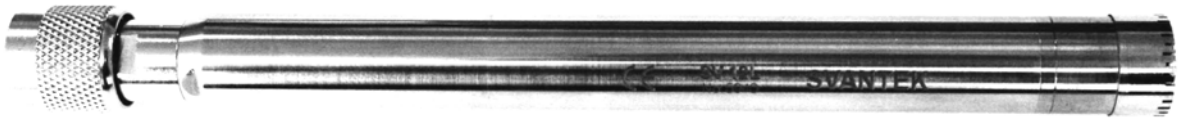


Рис. 4. Внешний вид измерительного микрофона

Подсоединение измерительного микрофона к измерительному модулю должно осуществляться следующим образом:

– без усилий вставить штекер разъема измерительного микрофона в разъем прибора;

– зафиксировать измерительный микрофон, закрутив блокировочное кольцо по часовой стрелке.

Нежелательно вращать измерительный микрофон вокруг оси во время соединения с прибором. Это может привести к механическому повреждению разъема.

Во время хранения измерительного микрофона на него должен быть надет защитный колпачок.

Внешний вид измерительного модуля с подключенным микрофоном показан на рис. 5.

Рис. 5. Внешний вид измерительного модуля с микрофоном

Измерительный вибродатчик

Измерительный вибродатчик является датчиком, предназначенным для измерения уровней виброакустических сигналов. Он также, как и микрофон, подключается непосредственно к измерительному модулю.

Внешний вид измерительного вибродатчика приведен на рис. 6.

Внешний вид измерительного модуля с подключенным вибродатчиком показан на рис. 7.

Следует очень аккуратно относиться к самому вибродатчику и его кабелю. Повреждение кабеля может служить причиной неправильных измерений.

Рис. 6. Внешний вид измерительного вибродатчика

Рис. 7. Внешний вид измерительного модуля с вибродатчиком

Измерительные дифференциальные усилители будут рассмотрены в одной из лабораторных работ, так как их использование при измерении сигналов акустоэлектрических преобразований имеет ряд особенностей.

3.2.2. Подсистема источника тестового акустического сигнала

В состав подсистемы источника тестового акустического сигнала входят:

– модуль источника тестового акустического сигнала «SZATG-03» в комплекте с зарядным устройством, антенной и соединительным кабелем;

– акустическая система со встроенным усилителем мощности;

– стойка-тренога для установки акустической системы.

Модуль источника тестового акустического сигнала «SZATG-03» используется для создания различных тестовых акустических сигналов при

проведении измерений звукоизоляционных и виброизоляционных параметров помещения, эффективности систем виброакустического зашумления и для других исследований.

Модуль источника тестового акустического сигнала «SZATG-03» генерирует следующие виды сигналов:

– непрерывный гармонический сигнал на частотах, соответствующих средним частотам третьоктавных полос в диапазоне от 20 до 20000 Гц;

– белый шум;

– розовый шум.

При использовании белого или розового шума, АЧХ сигнала может быть откорректирована с помощью программного эквалайзера подсистемы управления.

Управление модулем осуществляет подсистема управления дистанционно по радиоканалу. Внешний вид модуля тестового акустического сигнала приведен на рис. 8.

Рис. 8. Внешний вид модуля тестового акустического сигнала

Внешний вид передней панели модуля приведен на рис. 9.

Рис. 9. Внешний вид передней панели модуля тестового акустического сигнала

Акустическая система совместно с модулем «SZATG-03» предназначена для создания тестовых акустических сигналов во всех режимах работы комплекса «Спрут-7». В штатной комплектации используется активная акустическая система (со встроенным усилителем).

Внешний вид акустической системы в сборе приведен на рис. 10.

Рис. 10. Внешний вид акустической системы с подключенным модулем тестового акустического сигнала

3.2.3. Подсистема управления

В состав подсистемы управления входят:

– модуль сопряжения с управляющей ПЭВМ;

– портативная ПЭВМ (notebook);

– специальное программное обеспечение (СПО) «Спрут-7».

3.2.3.1. Модуль сопряжения с ПЭВМ

Модуль сопряжения с ПЭВМ осуществляет передачу команд управления в измерительный модуль и модуль источника тестового акустического сигнала «SZATG-03», а также прием результатов измерений от измерительного модуля. Подключение модуля сопряжения к ПЭВМ осуществляется через USB-порт. От USB-порта осуществляется и электропитание модуля сопряжения.

Внешний вид модуля сопряжения показан на рис. 11.

Рис. 11. Внешний вид модуля сопряжения

3.2.3.2. Специальное программное обеспечение «СПРУТ-7»

Специальное программное обеспечение (СПО) предназначено для управления измерительным модулем и модулем источника тестового акустического сигнала, получения результатов измерений, их обработки, отображения и сохранения в необходимом формате.

Запуск программы управления осуществляется из меню «ПУСК» – «Программы» – «Sprut-7». Через несколько секунд на экране ПЭВМ появится основное окно программы. Внешний вид главного окна программы управления показан на рис. 12.

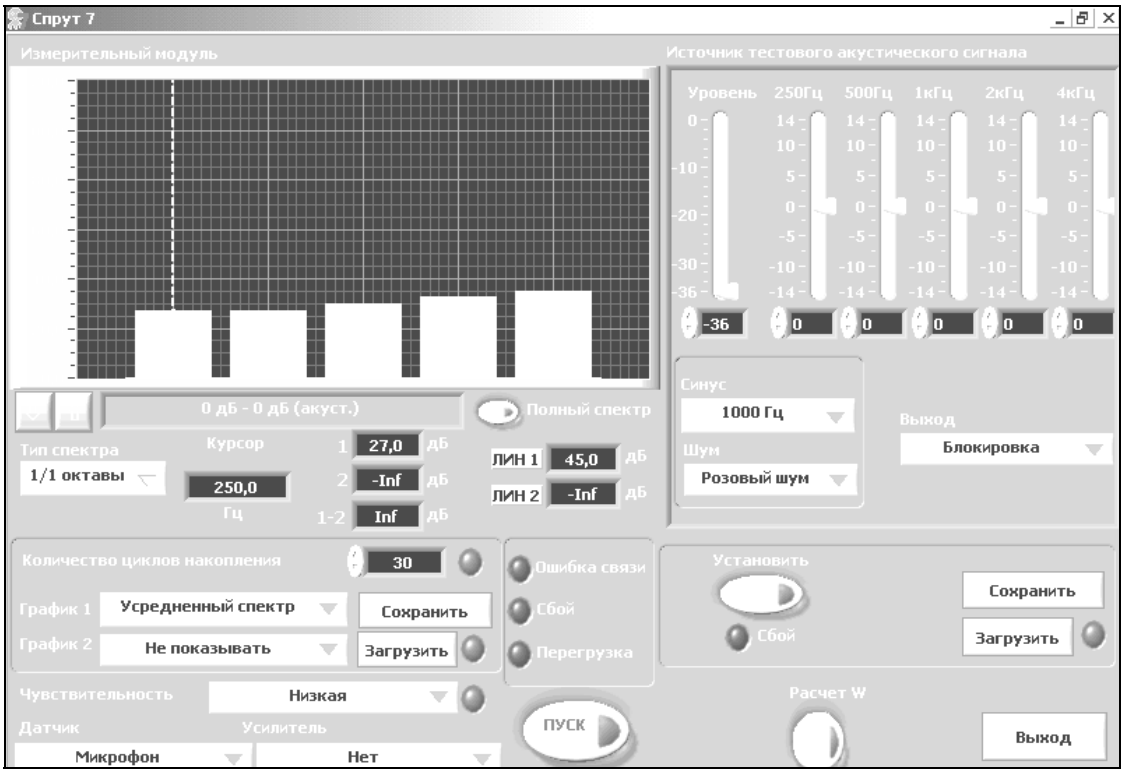
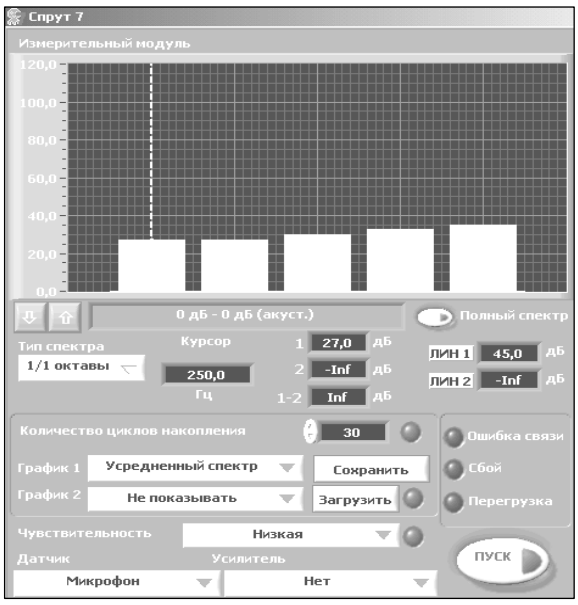


Рис. 12. Внешний вид главного окна СПО «СПРУТ-7»



Главное окно программы имеет две основные области:

– панель измерительного модуля;

– панель источника тестового акустического сигнала.

Панель измерительного модуля

Панель измерительного модуля предназначена для управления процессом измерений и отображения полученных данных. Панель измерительного модуля показана на рис. 13.

Рис. 13. Внешний вид панели измерительного модуля

Панель анализатора спектра

Предназначена для отображения спектра измеряемого сигнала, а также ранее сохраненных спектров. Внешний вид панели показан на рис. 14.

В зависимости от состояния переключателя «Полный спектр», на панели отображаются либо все составляющие октавного спектра в диапазоне частот от 1 Гц до 16 кГц, либо составляющие со средними частотами 250, 500, 1000, 2000 и 4000 Гц. С помощью кнопок  и  имеется возможность изменения пределов измерения в большую или меньшую сторону с шагом 20 дБ. На панели могут одновременно отображаться два спектра.

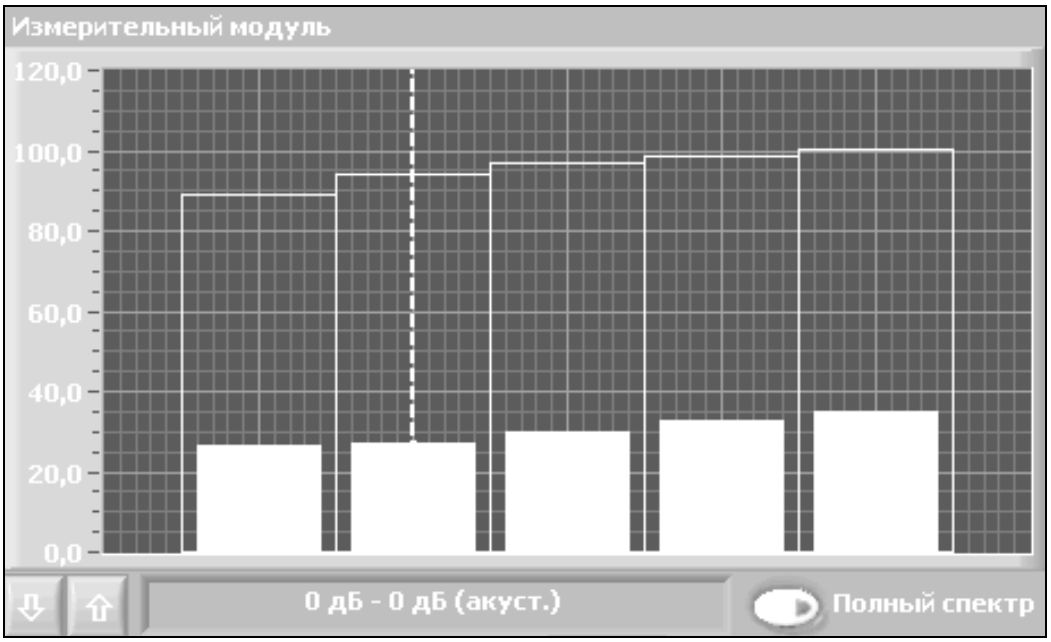
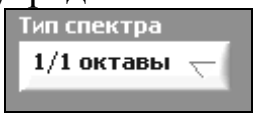


Рис. 14. Внешний вид панели анализатора спектра

Панель спектров

Панель спектров предназначена для управления отображением спектров, их сохранения, загрузки, определения интервала усреднения.

При помощи элемента управления «Тип спектра» 

можно выбрать способ отображения спектра: 1/1 октавы, либо 1/3 октавы. Выбор 1/3 октавы позволяет более подробно оценить спектральные составляющие входного сигнала. В этом случае каждая частотная октава дополнительно делится на 3 части. В практике акустических и виброакустических измерений принято оценивать входной сигнал по 5 октавам с центральными частотами 250, 500, 1000, 2000 и 4000 Гц. Режим 1/3 октавы, а также режим «Полный спектр» (переключатель режима «Полный спектр» находится на панели анализатора спектра) могут найти применение при проведении измерений сигналов акустоэлектрических преобразований.

На панели спектров могут быть одновременно отображены 2 спектра входного сигнала. Выбор этих спектров осуществляется следующим образом.

На панели с элементами управления спектрами, изображенной на рис. 15, с помощью элемента управления «График 1» пользователь определяет, что отображается в качестве спектра №1.

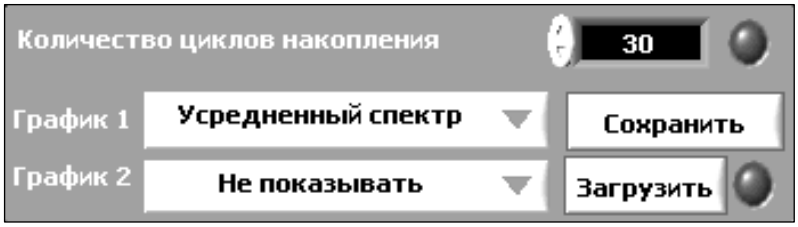


Рис. 15. Элементы управления спектрами

Перечень возможных вариантов выбора для элемента «График 1» приведен на рис. 16. Спектр №1 может быть сохранен в виде файла. Для этого используется кнопка «Сохранить».

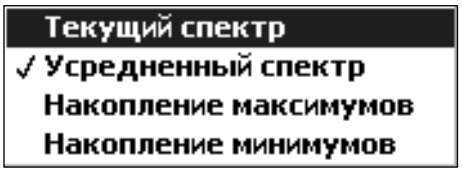


Рис. 16. Перечень возможных вариантов выбора для элемента «График 1»

С помощью элемента управления «График 2» пользователь определяет, что отображается в качестве спектра №2. Перечень возможных вариантов выбора приведен на рис. 17.

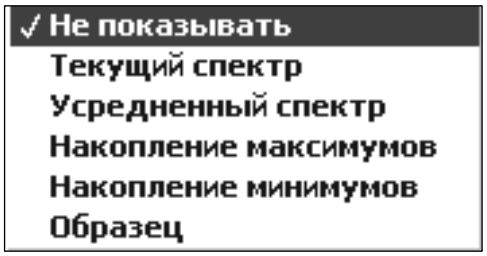


Рис. 17. Перечень возможных вариантов выбора для элемента «График 2»

В качестве образца может быть загружен из файла сохраненный ранее спектр. Для этого используется кнопка «Загрузить». Зеленый индикатор справа от кнопки загорается в случае успешного чтения файла.

На панели анализатора спектра «График 1» отображается столбцами зеленого цвета, «График 2» – незакрашенными столбцами с границей желтого цвета.

Элемент управления «Количество циклов накопления» позволяет оператору установить время сбора входной информации. Измерительный модуль обеспечивает измерение входного сигнала с интервалом в 1 сек, следовательно, цифровое значение, указанное в данном элементе управления, соответствует времени сбора входной информации в секундах. Спектр входного сигнала подвергается обработке выбранным в элементах управления «График 1», «График 2» способом («Текущий спектр», «Усредненный спектр» и т.д.) в течение указанного промежутка времени.

После запуска измерений индикатор справа от данного элемента управления погасает и загорается по истечении заданного времени, при

этом сбор информации не останавливается. Этот индикатор носит исключительно информативный характер, оператор должен самостоятельно останавливать и запускать измерения. Указанное по умолчанию значение количества циклов накопления – 30, выбрано не случайно. В нормативных и методических документах, регламентирующих акустические и виброакустические измерения, предписано осуществлять сбор информации (накопление минимумов и усреднение) именно в течение 30 секунд.

Панель курсора и интегральных уровней сигнала

Программное обеспечение позволяет определить величины сигналов и спектральные составляющие, измеренные измерительным модулем. Для этого используется так называемый курсор. Курсор отображается прерывистой вертикальной линией на панели анализатора спектра. Для перемещения курсора необходимо подвести к нему указатель мыши. При появлении символа ◄||►, нажать левую кнопку мыши, перетащить курсор на новое место и отпустить кнопку. Внешний вид панели курсора показан на рис. 18.

На панели отображается текущее положение курсора:

– частота;

– уровень соответствующей составляющей спектра №1;

– уровень соответствующей составляющей спектра №2;

– разность уровней составляющих спектра №1 и спектра №2.

Рис. 18. Внешний вид панели курсора

В правой части панели отображаются интегральные (в диапазоне частот от 0,8 до 20000 Гц) уровни сигналов для спектров №1 и №2.

Панель индикаторов

На панели индикаторов отображается информация об ошибках при проведении измерений. Внешний вид панели приведен на рис. 19.

Рис. 19. Внешний вид панели индикаторов

Индикатор «Ошибка связи» – загорается при отсутствии связи между модулем сопряжения с ПК и измерительным модулем. Обновляется 1 раз в секунду. Индикатор «Сбой» – загорается при возникновении ошибки связи в процессе измерений (при нажатой кнопке «Пуск»). При наличии такой ситуации измерения должны быть остановлены (кнопка «Пуск» отжимается). Индикатор «Перегрузка» сигнализирует о перегрузке входных цепей измерительного модуля.

Панель чувствительности

Элемент управления «Чувствительность» имеет три варианта выбора и позволяет установить верхний предел измерения сигнала. При значении «Низкая» верхний предел составляет 125 дБ; при значении «Средняя» – 110 дБ; при значении «Высокая» – 95 дБ. Внешний вид панели чувствительности с вариантами выбора показан на рис. 20.

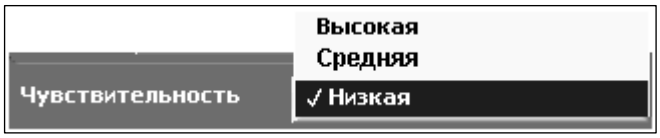


Рис. 20. Внешний вид панели чувствительности с вариантами выбора

Панель датчиков

На панели датчиков находятся органы управления, с помощью которых пользователь устанавливает тип используемых входных преобразователей. От состояния этих органов управления зависит то, как программное обеспечение будет интерпретировать полученные данные. Внешний вид панели датчиков с возможными вариантами выбора входных преобразователей приведен на рис. 21 с возможными вариантами выбора входных преобразователей.

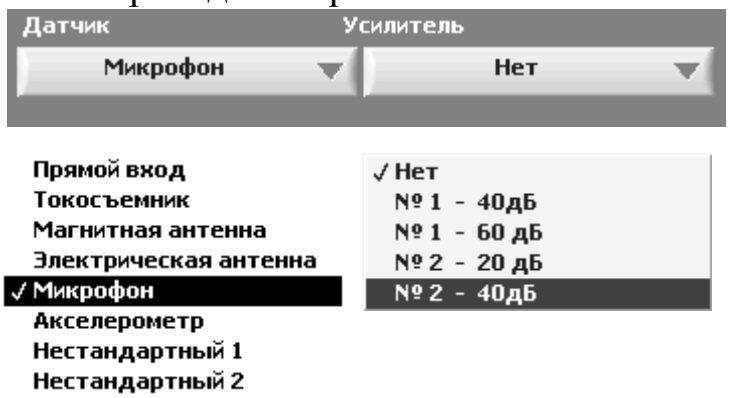


Рис. 21. Внешний вид панели датчиков

Кнопка «Пуск»

Нажатием кнопки ПУСК (рис. 22) запускается процесс измерений, повторным нажатием – останавливается.

Рис. 22. Внешний вид кнопки ПУСК до и после запуска измерений

Панель источника тестового акустического сигнала

Панель предназначена для управления источником тестового акустического сигнала. Внешний вид панели показан на рис. 23.

Рис. 23. Внешний вид панели источника тестового акустического сигнала

Основные элементы панели источника тестового акустического сигнала:

Панель эквалайзера

Панель предназначена для управления выходным уровнем сигнала модуля источника тестового акустического сигнала и корректировки его АЧХ. Погрешность установки уровня источника тестового акустического сигнала не нормируется, шкалы регуляторов носят условный характер. Уровень и АЧХ сигнала определяется измерительным модулем. Внешний вид панели эквалайзера изображен на рис. 24.

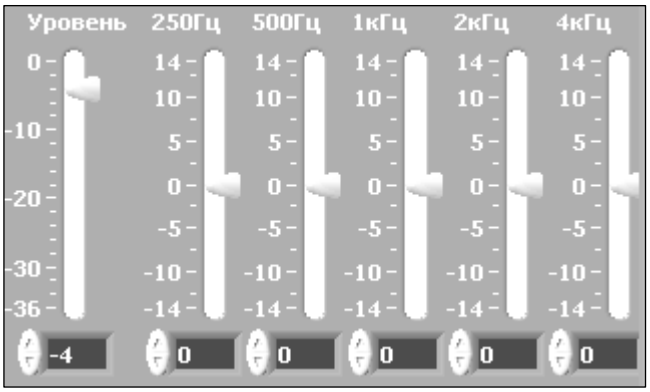


Рис. 24. Внешний вид панели эквалайзера

Настройки эквалайзера активизируются в том случае, если на панели выходного сигнала в качестве выходного сигнала выбран «Шум с эквалайзером».

Панель выходного сигнала

Панель выходного сигнала предназначена для дистанционного управления модулем источника тестового акустического сигнала «SZATG-03». Элемент управления «Синус» предназначен для установки частоты генерируемого выходного синусоидального сигнала. Частота выбирается из списка. Элемент управления «Шум» позволяет пользователю выбрать тип выходного шумового сигнала (белый, розовый шум, шум с эквалайзером). Элемент управления «Выход» позволяет пользователю выбрать тип выходного сигнала (синусоидальный, шум, шум с эквалайзером), либо его заблокировать. Внешний вид панели выходного сигнала с возможными вариантами выбора приведен на рис. 25. Сигнал на выходе модуля тестового акустического сигнала появляется сразу же после выбора элементом управления «Выход» выбранного вида сигнала.

Рис. 25. Внешний вид панели выходного сигнала с возможными вариантами выбора

Дополнительная панель

Внешний вид дополнительной панели управления приведен на рис. 26. Нажатием кнопки «Сохранить» можно записать в файл текущие настройки

источника тестового акустического сигнала, а нажатием кнопки «Загрузить» – прочитать из файла и установить сохраненные ранее настройки.

Зеленый индикатор справа от кнопки загорается в случае успешного чтения файла. Нажатие на кнопку «Установить» позволяет повторно передать настройки модулю источника тестового акустического сигнала в случае сбоя связи.

Рис. 26. Внешний вид дополнительной панели управления

Индикатор «Сбой» загорается в случае, если в процессе передачи настроек возникла ошибка связи.

Кнопка «Расчет W» запускает дополнительную программу, рассчитывающую по полученным данным степень звукоизоляции (виброизоляции) испытанной ограждающей конструкции. Выходным результатом работы данной программы является некое число W – показатель противодействия акустической речевой разведке, он же – словесная разборчивость речи. Однако этот показатель имеет значение лишь при работах, связанных с защитой государственной тайны, поэтому в данной и последующих лабораторных работах нами применяться не будет.

4. Задание на выполнение работы

4.1. Изучить теоретические вопросы, изложенные в п. 2 настоящей лабораторной работы.

4.2. Подготовить комплекс «СПРУТ-7» для измерений акустических величин.

4.3. Изучить работу комплекса и специального программного обеспечения.

4.4. Оформить отчет по лабораторной работе.

4.5. Ответить на контрольные вопросы.

5. Порядок выполнения работы

5.1. Подготовить комплекс «Спрут-7» для проведения акустических измерений.

Для подготовки комплекса необходимо выполнить следующие действия:

– Подключить модуль сопряжения к ПЭВМ.

− Подключить измерительный микрофон к измерительному модулю.

− Подключить антенну к измерительному модулю.

− Включить питание измерительного модуля. На ЖК-индикаторе модуля в правом верхнем углу отобразится уровень заряда батарей модуля. При необходимости замените батареи измерительного модуля.

− Подключить источник тестового акустического сигнала к акустической системе.

– Включить питание акустической системы.

– Включить питание модуля источника тестового акустического сигнала (для этого необходимо удерживать кнопку включения 1-2 секунды. Когда модуль включится, светодиод на передней панели загорится зеленым светом. Выключение модуля выполняется аналогичным образом).

– Запустить программное обеспечение для управления комплексом. При запуске ПО возможно, что на экране появится окно с ошибкой «Нет связи с измерительным модулем». Это значит, что расстояние между измерительным модулем и модулем сопряжения слишком мало, как правило менее 2 метров, что приводит к ошибкам в работе радиоканала. Необходимо отнести измерительный модуль на большее расстояние и перезапустить программу управления.

Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:

– тип входного датчика – микрофон;

– кнопка «Полный спектр» отжата;

– чувствительность – низкая;

– фильтры 1/1 октавы;

– панель источника тестового сигнала – активна;

– уровень выходного сигнала источника тестового акустического сигнала – минимум;

–выход – блокировка.

5.2. Изучить работу специального программного обеспечения

5.2.1. Для запуска процесса измерений на панели управления измерительным модулем нажмите кнопку «Пуск». Установите время усреднения – 2 сек. На панели анализа спектра должен отобразиться текущий спектральный состав акустического фона в помещении. С помощью элементов управления «Полный спектр» и «Тип спектра» добейтесь отображения максимально подробного спектра входного сигнала. Входным сигналом в данном случае является фоновая акустическая обстановка в помещении.

5.2.2. На «графике 1» включите отображение текущего спектра, на «графике 2» включите отображение усредненного спектра, затем накопление минимумов и накопление максимумов. Поясните полученные результаты.

5.2.3. Установите время усреднения 30 сек. Для «графика 1» включите режим «Накопление минимумов» и заново проведите набор входной информации. Для этого необходимо остановить измерения кнопкой «СТОП» и заново запустить их кнопкой «ПУСК». Через 30 сек измерений загорится индикатор справа от элемента «Количество циклов накопления». Это означает, что прошло 30 сек. Остановите измерения. Сохраните накопленный спектр в файл с произвольным именем. Попробуйте загрузить данный файл спектра как исходный для «графика 2». Убедитесь, что загрузка произошла

верно и «график 2» идентичен «графику 1». Запустив измерения заново можно видеть, что «график 1» отображает текущий спектр входного сигнала, а «график 2» – загруженный спектр. Такая возможность программного обеспечение позволяет оценивать изменение акустической обстановки в помещении в различные моменты времени.

5.2.4. Расположите акустическую систему (АС) на штативе на высоте примерно 1,5 м от пола. Измерительный модуль с микрофоном расположите напротив диффузора динамика акустической системы, перпендикулярно ему. Расстояние между микрофоном и АС – 30 см.

Запустите измерения кнопкой «ПУСК». В панели управления модулем акустического сигнала с помощью элемента «ВЫХОД» установите «Белый шум». С помощью регулятора «Уровень» начинайте увеличивать громкость шума, воспроизводимого АС, до уровня, еще не мешающего окружающим, но уже достаточного для уверенного отображения спектра. Запишите значение уровня установленного выходного сигнала. Убедитесь, что спектр акустического сигнала, воздействующего на измерительный микрофон и отображаемого на панели анализа спектров, близок к спектру белого шума.

5.2.5. Переключая при помощи элементов управления модулем тестового акустического сигнала различные режимы работы «Синус», «Розовый шум», наблюдайте изменение спектрального состава сигнала, излучаемого АС. Для режима «Синус – 1000 Гц» зарисуйте полученный спектр, поясните полученный результат. Переключите комплекс в режим «1/1 октавы», выключите переключатель «Полный спектр». Убедитесь, что в панели анализа спектров отображается 5 октавных полос акустического сигнала. Проведите измерения уровней звукового давления в каждой из 5 октавных полосах для режима «Синус – 1000 Гц», а также интегрального уровня звукового сигнала. Проведите те же измерения для режима «Белый шум». Запишите полученные результаты.

5.2.6. Включите тип выхода – «Шум с эквалайзером». Изменяя уровень спектральных составляющих на панели эквалайзера убедитесь, что излучаемый АС шум меняет тембровую окраску, что подтверждается формой спектра звукового сигнала, наблюдаемой в панели анализа спектров.

5.2.7. Выключите выход модуля тестового акустического сигнала при помощи элемента управления «ВЫХОД» – «Блокировка».

5.3. Завершение работы

Выключите комплекс «СПРУТ-7». Для этого:

− завершите работу с программой;

− выключите АС выключателем питания;

− выключите модуль тестового акустического сигнала;

− выключите измерительный модуль;

− отсоедините измерительный микрофон, оденьте защитный колпачок, упакуйте микрофон в предназначенный пакет.

− отключите модуль сопряжения;

− сложите все компоненты комплекса в сумку.

6. Содержание отчета

В отчете привести задание на выполнение лабораторной работы, схему соединения компонентов комплекса «СПРУТ-7» при анализе акустических сигналов, виброакустических сигналов, рисунки спектров и измеренные значения звукового давления, полученные в ходе выполнения работы, ответы на контрольные вопросы.

7. Контрольные вопросы

7.1. Что представляет собой речевой сигнал?

7.2. Что представляет собой звуковое давление?

7.3. В каких единицах измеряется звуковое давление?

7.4. Перечислите типовые подсистемы современного программно-аппаратного комплекса для акустических измерений.

7.5. Какие каналы утечки речевой информации можно выявить и оценить их характеристики с помощью комплекса «Спрут-7»?

7.6. Почему в акустических измерениях принято деление спектра речевого сигнала на небольшое число (5) октав?

7.7. Перечислите возможности программно-аппаратного комплекса «Спрут-7».

7.8. Что понимают под прямым акустоэлектрическим преобразованием?

7.9. С какой целью в комплексе «Спрут-7» заложена возможность генерации белого шума?

7.10. Какого вида сигналы генерирует источник тестового акустического сигнала «SZATG-03»?

Лабораторная работа №5

ОЦЕНКА ЗАЩИЩЕННОСТИ ОГРАЖДАЮЩИХ КОНСТРУКЦИЙ ПОМЕЩЕНИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО АКУСТИЧЕСКОМУ КАНАЛУ КОМПЛЕКСОМ «СПРУТ-7»

1. Цель работы

Изучить порядок применения комплекса «Спрут-7» при оценке защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу. Научиться рассчитывать коэффициенты звукоизоляции ограждающих конструкций помещения и оформлять результаты измерений.

2. Краткие теоретические сведения

Применительно к акустическому каналу утечки речевой информации в защищаемом помещении источником информации является, как правило, человек, средой распространения – воздух. Задача разведки – получить защищаемую речевую информацию. Для этого могут применяться различные технические средства. Однако получение информации сопряжено с некоторыми трудностями: ограждающие конструкции помещения вызывают затухание акустического сигнала, шумовая обстановка в точке съема информации может не позволить распознать принятую речь. Эти факторы при защите речевой информации используют соответственно при пассивной и активной защите информации техническими средствами.

Основная идея пассивных средств защиты информации – это снижение соотношения сигнал/шум в возможных точках перехвата информации за счет снижения уровня информативного сигнала. Для этого при выборе ограждающих конструкций при проектировании помещений необходимо руководствоваться следующими правилами:

− в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;

− потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

− в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т.п.);

− применение тройного остекления окон на двух рамах, закрепленных на отдельных коробках. При этом на внешней раме устанавливаются сближенные стекла, а между коробками укладывается звукопоглощающий материал;

− в качестве дверей целесообразно использовать двойные двери с тамбуром, при этом дверные коробки должны иметь вибрационную развязку друг от друга.

Основную опасность, с точки зрения возможности утечки информации по акустическому каналу, представляют различные строительные тоннели и короба, предназначенные для осуществления вентиляции и размещения различных коммуникаций, так как они представляют собой акустические волноводы.

В случае дефицита акустической изоляции ограждающих конструкций помещения (стен, перегородок, ограничивающих помещение, дверей) применяются методы активной защиты, позволяющие ухудшить соотношение сигнал/шум в точке вероятного съема информации за счет создания фонового шума. Как правило, это специально разработанные устройства. Это могут быть генераторы шума, генераторы речеподобной помехи, словом те устройства, которые при помощи акустических излучателей обеспечивают такую шумовую обстановку в месте возможного съема информации, что получение осмысленной информации становится просто невозможным. Акустические излучатели могут располагаться в тамбурах входных дверей (в случае, если последние не обеспечивают требуемого затухания), в смежных помещениях (если перегородки также не удовлетворяют требованиям по звукоизоляции), в воздуховодах и вентиляционных коробах, в месте выхода которых из защищаемого помещения возможен съем информации.

В данной работе применяется методика инструментально-расчетной оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому, разработанная Гостехкомиссией России.

Метод оценки защищенности помещения от утечки речевой информации по акустическому каналу заключается в определении коэффициентов звукоизоляции ограждающих конструкций (ОК) в октавных полосах частот со средними частотами 250, 500, 1000, 2000, 4000 Гц и последующим сопоставлением полученных коэффициентов с их нормативными значениями.

3. Задание на выполнение работы

3.1. Изучить особенности заданной ограждающей конструкции (ОК). Оценить их возможное влияние на степень звукоизоляции.

3.2. Подготовить комплекс «Спрут-7» для проведения акустических измерений.

3.3. Провести измерения степени звукоизоляции заданной ограждающей конструкции.

3.4. Оформить протокол контроля и дать рекомендации по устранению дефектов ОК и/или применению дополнительных мер защиты.

4. Порядок выполнения работы

4.1. Проведите осмотр и анализ архитектурно-планировочных решений помещения с целью определения характера и конструктивных особенностей ОК и инженерных коммуникаций (ИК) (воздуховоды, вент. короба и т.п.), особенностей смежных помещений и прилегающих к помещению уличных пространств.

4.2. Составьте план-схему помещения, отметьте на ней предложенную для оценки звукоизоляции ОК.

4.3. Опишите заданную ОК, поясните возможные пути утечки речевой информации через нее.

4.4. На плане помещения и предложенной ОК выберите точки контроля (контрольные точки (КТ)). Контрольные точки выбираются в местах, наиболее опасных с точки зрения перехвата информации. Это, например, точка перед входной дверью, за окном, точки в смежных помещениях, точки внутри или снаружи инженерных коммуникаций (вентиляционные короба, воздуховоды и т.п.).

4.5. Подготовьте комплекс «Спрут-7» для проведения акустических измерений. Для этого:

− Подключите модуль сопряжения к ПЭВМ.

− Подключите измерительный микрофон к измерительному модулю. Подключите антенну к измерительному модулю. Включите питание измерительного модуля. На ЖК-индикаторе модуля в правом верхнем углу отобразится уровень заряда батарей модуля. При необходимости замените батареи измерительного модуля.

− Подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сигнала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.

− Запустите программное обеспечение для управления комплексом. Убедитесь, что:

− тип входного датчика – микрофон;

− кнопка «Полный спектр» отжата;

− чувствительность – низкая;

− фильтры 1/1 октавы;

− панель источника тестового сигнала – активна;

− уровень выходного сигнала источника тестового акустического сигнала – минимум;

− выход – блокировка.

4.6. Проведение измерений

Суть измерения коэффициентов звукоизоляции состоит в следующем:

− измеряется уровень так называемого тестового сигнала, излучаемого акустической системой (АС) комплекса;

− измеряется уровень фоновых шумов в контрольной точке;

− измеряется уровень акустического тестового сигнала в контрольной точке;

− рассчитывается коэффициент звукоизоляции;

− делается вывод о достаточности/недостаточности звукоизолирующей способности ОК.

По окончании измерении оформляется протокол установленной формы.

4.6.1. Измерение уровня тестового сигнала

Для измерения уровня тестового сигнала необходимо:

− расположить акустическую систему на высоте 1,5 м от пола на штативе;

− расположить измерительный микрофон напротив диффузора динамика акустической системы, перпендикулярно ему. Расстояние между микрофоном и АС – 1 м;

− используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – усреднение спектра; количество циклов накопления – 30. Нажмите кнопку «Пуск». В окне анализатора спектра должен отобразиться текущий спектральный состав акустического фона в помещении. В панели управления модулем акустического сигнала с помощью элемента «Выход» установите «Белый шум». С помощью регулятора уровня в панели источника тестового акустического сигнала начинайте увеличивать громкость шума, воспроизводимого АС. Добейтесь такого уровня, чтобы интегральный уровень звука был не менее 70 дБ. При измерениях в реальных условиях может потребоваться и больший уровень сигнала с тем, чтобы уменьшить влияние посторонних шумов на результат измерения. В окне анализатора спектра вы увидите спектр белого шума, разделенный на 5 октав, принятых при проведении акустических измерений. Через 30 сек, после того, как загорится зеленый индикатор справа от элемента «Количество циклов накопления», нажмите кнопку «Стоп». В окне управления модулем акустического сигнала установите режим «Выход» – «Блокировка». В течение всех последующих измерений не изменяйте настройки уровня источника тестового акустического сигнала и не регулируйте уровень громкости на АС.

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2, в графу $L_{c1\,i}$, где i – номер октавной полосы (от 1 до 5).

4.6.2. Измерение уровня фонового шума

Для измерения уровня фонового шума в контрольной точке выполните следующие действия:

− расположите измерительный микрофон в контрольной точке на расстоянии 0,5 м от плоскости оцениваемой ОК;

− используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – накопление минимумов, количество циклов накопления – 30. Нажмите кнопку «Пуск». В панели анализатора спектра будут отображаться минимальные значения спектральных составляющих фоновой обстановки. Измерения необходимо проводить при минимальных уровнях внешних шумов (при отсутствии персонала, при выключенных системах кондиционирования и вентиляции и пр.). Через 30 сек, после того, как загорится зеленый индикатор справа от элемента «Количество циклов накопления», нажмите кнопку «Стоп».

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2, в графу $L_{ш\,i}$, где i – номер октавной полосы (от 1 до 5).

4.6.3. Измерение уровня акустического сигнала в контрольной точке

При измерении степени звукоизоляции ОК АС должна быть направлена в сторону ОК и находиться на расстоянии 1,5 м от нее. Ось апертуры АС направляется в сторону ОК по нормали к ее поверхности. Если ОК является пол (потолок), то АС размещается в центре помещения на высоте 1…1,5 м от пола. Ось апертуры направляется соответственно в пол или потолок по нормали к поверхности ОК. Расположенный с другой стороны ОК измерительный микрофон, должен находиться на той же высоте, что и АС (1,5 м) на расстоянии 0,5 м от плоскости ОК.

В панели управления модулем акустического сигнала с помощью элемента «тип выхода» установите «Белый шум». Запустите сбор информации, нажатием кнопки «Пуск» на панели управлении измерительным модулем. Через 30 сек нажмите кнопку «Стоп». Отключите генерацию шума (в окне управления модулем акустического сигнала установите режим «Выход» – «Блокировка»).

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2 в графу $L_{(с+ш)\,i}$, где i – номер октавной полосы (от 1 до 5).

4.6.4. Расчет коэффициентов звукоизоляции

Рассчитайте октавные уровни акустического сигнала $L_{с2i}$ по формулам (1):

$$L_{с2i} = \begin{cases} L_{(с+ш)_i} & \text{при } L_{(с+ш)_i} - L_{ш_i} \geq 10 \\ L_{(с+ш)_i} - \Delta & \text{при } L_{(с+ш)_i} - L_{ш_i} < 10 \end{cases}, \quad (1)$$

где Δ – поправка в дБ, определяется из табл. 4.1.

Таблица 4.1

$L_{(с+ш)\,i}$	> 10	6…10	4…6	3	2	1	0,5
Δ, дБ	0	1	2	3	4	7	10

Запишите рассчитанные значения $L_{с2i}$ в табл. 4.2.

Октавные уровни звукоизоляции Q_i рассчитываются по формуле (2):

$$Q_i = L_{с1_i} - L_{с2_i} \quad (2)$$

Запишите рассчитанные значения Q_i в табл. 4.2.

Сравните полученные значения Q_i с требуемыми нормативными значениями, приведенными в табл. 4.3. Если хотя бы один из коэффициентов звукоизоляции меньше, чем нормированное значение, делается вывод о недостаточности звукоизоляции и следовательно о незащищенности помещения от утечки речевой информации.

Таблица 4.2

Результаты расчетов октавных коэффициентов звукоизоляции

Номер октавной полосы, i	Измеренный уровень акустического шума в контрольной точке $L_{ш\,i}$, дБ	Уровень тестового сигнала L_{c1i}, дБ	Уровень измеренного суммарного акустического сигнала и акустического шума в контрольной точке $L_{(c+ш)\,i}$, дБ	Расчетный уровень акустического сигнала в контрольной точке L_{c2i}, дБ	Октавные уровни звукоизоляции в контрольной точке Q_i, дБ
Контрольная точка №					
1					
2					
3					
4					
5					

Таблица 4.3

Нормативные значения коэффициента звукоизоляции

Место возможного перехвата речевой конфиденциальной информации из помещения		Нормативное значение октавного коэффициента звукоизоляции, дБ	
		для помещений, не оборудованных системами звукоусиления	для помещений, оборудованных системами звукоусиления
Смежные помещения		46	60
Уличное пространство	Улица без транспорта	36	50
	Улица с транспортом	26	40

4.7. Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

- завершите работу с программой;
- выключите АС выключателем питания;
- выключите модуль тестового акустического сигнала;
- выключите измерительный модуль;
- отсоедините измерительный микрофон, оденьте защитный колпачок, упакуйте его в предназначенный пакет.
- отключите модуль сопряжения;
- сложите все компоненты комплекса в сумку.

5. Содержание отчета

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации (рекомендуемая форма протокола приведена в приложении), а также ответы на контрольные вопросы.

6. Контрольные вопросы

6.1. Чем принципиально отличаются методы пассивной и активной защиты речевой информации?

6.2. Почему уровни фонового шума в контрольной точке необходимо измерять в условиях минимальной зашумленности: при отсутствии транспорта, персонала и т.д.?

6.3. Почему при проведении измерений строго оговариваются расстояния между элементами измерительного тракта (акустической системы, ограждающей конструкцией и микрофоном)?

6.4. Что представляет собой сферическая звуковая волна?

6.5. Как подразделяются по типу огибающей амплитудно-частотного спектра шумы?

6.6. Как подразделяются шумы в зависимости от ширины частотного спектра

6.7. Что называют звуковой маскировкой?

6.8. Что понимают под разборчивостью речи?

6.9. Каким выражением определяется звукоизоляция перегородки?

6.10. Если хотя бы один из октавных коэффициентов звукоизоляции Q_i будет меньше, чем нормированное значение, то какой делается вывод?

Приложение

Рекомендуемая форма протокола инструментально-расчетной оценкизащищенности помещения от утечки речевой конфиденциальной информации

ПРОТОКОЛ
инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации

1. Объект оценки (наименование помещения, адрес).

2. Назначение помещения и его краткое описание (расположение помещения, план-схема помещения).

3. Вид оценки – аттестационный контроль.

4. Вид оцениваемого канала перехвата речевой информации – акустический.

5. Оцениваемые ограждающие конструкции и элементы технических систем (окно, дверь, стены, пол, потолок, вент. канал и т.д.).

6. Описание применяемых мер и средств защиты (уплотненные притворы дверей, шторы, организационные меры и т.п.).

7. Перечень средств измерений и вспомогательного оборудования (наименование, тип, заводской номер, дата очередной поверки).

8. Перечень нормативных и методических документов, используемых при оценке защищенности.

(Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, 2002).

9. Результаты измерений и расчетов звукоизоляции.

10. Заключение о выполнении требований по защите (выполняются, не выполняются).

Оценку защищенности выполнил

_____ _____

(наименование должности, инициалы, фамилия) (личная подпись)

Дата

Лабораторная работа №6

ОЦЕНКА ЗАЩИЩЕННОСТИ ОГРАЖДАЮЩИХ КОНСТРУКЦИЙ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ КОМПЛЕКСОМ «СПРУТ-7»

1. Цель работы

Изучить методику применения комплекса Спрут-7 при оценке защищенности ограждающих конструкций помещения от утечки информации по виброакустическому каналу. Научиться рассчитывать коэффициенты виброизоляции ограждающих конструкций помещения и оформлять результаты измерений.

2. Краткие теоретические сведения

Речь, вызывающая акустические сигналы, представляет собой механические колебания воздушной среды. Попадая на твердые поверхности (стены, перегородки, трубы систем отопления и т.д.), они преобразуются в так называемый структурный звук – механические колебания в твердом теле. Механические колебания стен, перекрытий, трубопроводов и т.п. передаются на значительные расстояния со слабым затуханием и хорошо перехватываются приемными устройствами.

Распространение структурных волн в инженерных конструкциях здания характеризуется:

− затуханием вследствие их расхождения и поглощения (перехода энергии в тепло);

− отражением на границах раздела сред (например, составные стены из разного материала, места разветвления, углы) и т.п.;

− преобразованием типов волн (например, изгибных в продольные);

− излучением в воздушную среду.

Опасность виброакустического канала утечки речевой информации состоит в большой и непредсказуемой дальности распространения звуковых волн, преобразованных в структурные колебания элементов инженерных коммуникаций (ИК). Экспериментальные исследования показали возможность перехвата речевой информации с высоким качеством в зданиях из железобетона через один – два этажа (затухание 0,1–0,15 дБ/м), по трубопроводам – через два-три этажа (затухание 5–15 дБ/этаж).

Одновременно с этим следует отметить, что съем виброакустической информации, как правило, невозможен без использования специальных технических средств, например, стетоскопов.

Частным случаем виброакустического канала можно считать оптико-электронный канал утечки информации. Источником информации в этом случае являются механические колебания стекол окон помещения. При помощи так называемых лазерных микрофонов речевая информация со

стекол может быть получена на расстояниях до сотен метров. Очевидно, что внутренние стекла окна помещения имеют большую амплитуду колебаний, чем наружные, однако съем информации с них сложнее. Поэтому в настоящее время не существует четкого понимания о степени опасности внутренних и наружных стекол в плане съема информации и их защита осуществляется одинаковым образом.

Шумы и помехи, имеющиеся в месте возможного съема информации, вызываются многочисленными источниками – автомобильным транспортом, работой механических устройств, технических средств в помещениях, разговорами в смежных помещениях и т.п.

Методы защиты речевой информации от утечки по виброакустическому и акустическому каналам основаны на уменьшении соотношения сигнал/шум в точке вероятного съема информации. При этом различают пассивные и активные методы.

Пассивные методы направлены на уменьшение уровня информативного сигнала за счет улучшения виброизоляции инженерных конструкций.

Активные методы основаны на увеличении уровня шума по отношению к естественному (фоновому) и реализуются с помощью технических средств, основу которых составляют различные генераторы шума, формирующие виброшум в ограждающих конструкциях или инженерных коммуникациях.

В данной работе применяется методика инструментально-расчетной оценки защищенности помещений от утечки речевой конфиденциальной информации по виброакустическому каналу, разработанная Гостехкомиссией России.

Метод оценки защищенности помещения от утечки речевой информации по виброакустическому каналу заключается в определении коэффициентов виброизоляции ограждающих конструкций (ОК) в октавных полосах частот со средними частотами 250, 500, 1000, 2000, 4000 Гц и последующим сопоставлением полученных коэффициентов с их нормативными значениями.

3. Задание на выполнение работы

3.1. Изучить особенности заданных ограждающих конструкций или инженерных коммуникаций.

3.2. Подготовить комплекс «Спрут-7» для проведения виброакустических измерений.

3.3. Провести измерения степени виброизоляции заданных ОК или ИК.

3.4. Оформить протокол контроля и дать рекомендации по применению дополнительных мер защиты.

4. Порядок выполнения работы

4.1. Проведите осмотр и анализ заданной ОК/ИК помещения с целью определения возможного направления утечки информации.

4.2. Составьте план схему помещения, отметьте на ней предложенную для оценки виброизоляции ОК/ИК.

4.3. На плане помещения и предложенной ОК выберите точки контроля (контрольные точки (КТ)). Контрольные точки выбираются в местах, наиболее опасных с точки зрения перехвата информации.

Выбор места расположения контрольных точек производится по следующим правилам:

− на подводимой к проверяемому помещению трубопроводной коммуникации контрольные точки располагаются на расстоянии 0,3…0,5 м от места ее выхода из проверяемого помещения. Если это невозможно, то необходимо найти ближайшую к помещению доступную для съема информации точку;

− при наличии вентиляционного короба, подводимого к помещению, две-три контрольные точки располагаются на поверхности воздухопровода на расстоянии 0,3…0,5 м от места выхода из проверяемого помещения;

− на сплошном однородном ограждении (стена, перекрытие) контрольные точки располагаются в соответствии с рис. 1, по диагонали от центра к углу с шагом 0,3…1 м. Крайние точки располагаются на расстоянии не менее 0,25 м от вершин углов ОК;

− на сплошном неоднородном ограждении, например стене, отдельные участки которой имеют различную толщину или выполнены из различных материалов, контрольные точки располагаются в соответствии с предыдущей рекомендацией по отношению к каждому однородному участку;

− на остеклении оконных проемов контрольные точки располагаются в соответствии с рис. 1 для каждой рамы окна и каждого участка остекления;

− на дверном проеме контрольные точки располагаются в соответствии с рис. 1, а также на поверхности коробки двери по ее периметру.

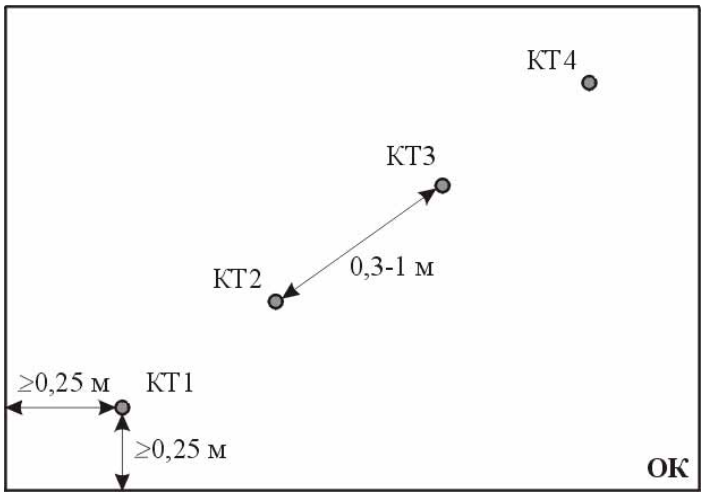


Рис. 1. Схема расположения контрольных точек на однородном участке ограждающей конструкции

4.4. Подготовьте комплекс «Спрут-7» для проведения виброакустических измерений. Для этого:

− подключите модуль сопряжения к ПЭВМ;

− подключите измерительный вибродатчик к измерительному модулю. Подключите антенну к измерительному модулю. Включите питание изме-

рительного модуля. На ЖК-индикаторе модуля в правом верхнем углу отобразится уровень заряда батарей модуля. При необходимости замените батареи измерительного модуля.

− подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сигнала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.

− запустите программное обеспечение для управления комплексом. Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:

− тип входного датчика – акселерометр;

− кнопка «Полный спектр» отжата;

− чувствительность – низкая;

− фильтры 1/1 октавы;

− панель источника тестового сигнала – активна;

− уровень выходного сигнала источника тестового акустического сигнала – минимум;

− тип выхода – блокировка.

4.5. Проведение измерений

Суть измерения коэффициентов виброизоляции состоит в следующем:

− производится измерение так называемого тестового вибросигнала непосредственно на поверхности ОК или контролируемого элемента ИК внутри помещения. Исходный тестовый акустический сигнал излучается акустической системой (АС) комплекса;

− измеряется уровень фоновых виброшумов в контрольной точке;

− измеряется уровень вибросигнала на поверхности ОК/ИК в контрольной точке. Исходный тестовый акустический сигнал излучается акустической системой комплекса;

− рассчитывается коэффициент виброизоляции;

− делается вывод о достаточности/недостаточности виброизолирующей способности ОК.

По окончании измерении оформляется протокол установленной формы.

4.5.1. Измерение уровня тестового вибросигнала

Для измерения уровня тестового сигнала необходимо:

− расположить акустическую систему на высоте 1,5 м от пола на штативе на расстоянии 1 м от обследуемой ОК/ИК (при всех остальных измерениях АС должна располагаться на расстоянии 1,5 м от обследуемой ОК/ИК). Ось апертуры АС направляется в сторону ОК по нормали к ее поверхности. Если ОК является пол (потолок), то АС размещается в центре помещения на высоте 1…1,5 м от пола. Ось апертуры направляется соответственно в пол или потолок по нормали к поверхности ОК;

– закрепить измерительный вибродатчик на заданной ОК/ИК. Датчик закрепляется по возможности напротив диффузора динамика акустической системы, перпендикулярно ему. В случае с оконным остеклением, датчик необходимо прикрепить в центре самого большого стекла изнутри помещения и установить АС по возможности на высоте вибродатчика.

Крепление вибродатчика на ОК/ИК должно быть механически жестким. Для этого в комплект комплекса входят различные крепежные элементы: хомут для крепления вибродатчика на трубы системы отопления и водоснабжения, площадка для крепления на стекла окон, шпильки с резьбой для стен. Внешний вид крепежных элементов и примеры крепления приведены в приложении А.

На хомут для труб и дюбели вибродатчик закрепляется резьбовым соединением. Для прикрепления вибродатчика к стеклу необходимо закрепить на вибродатчике площадку для крепления на окна, нанести на площадку немного пчелиного воска (прилагается к комплексу), разогреть воск при помощи зажигалки или спички, и пока воск не остыл приклеить площадку вместе с вибродатчиком к стеклу в выбранной контрольной точке. На подоконник под местом установки вибродатчика необходимо положить какой-нибудь предмет, который предохранит вибродатчик от удара при падении при неудачном приклеивании, либо принять другие меры для исключения падения датчика;

– используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – усреднение спектра, количество циклов накопления – 30. Нажмите кнопку «Пуск». В окне анализатора спектра должен отобразиться текущий спектральный состав виброакустического фона в помещении. На панели управления модулем акустического сигнала с помощью элемента «Выход» установите «Белый шум». С помощью регулятора уровня на панели источника тестового акустического сигнала начинайте увеличивать громкость шума, воспроизводимого АС. Добейтесь такого уровня, чтобы интегральный уровень вибросигнала был не менее 90 дБ (при измерениях на стеклах уровень может доходить до 100 дБ и более). В окне анализатора спектра вы увидите спектр белого шума, разделенный на 5 октав, принятых при проведении акустических измерений. Через 30 сек, после того, как загорится зеленый индикатор справа от элемента «Количество циклов накопления», нажмите кнопку «Стоп». В окне управления модулем акустического сигнала установите режим «Выход» – «Блокировка». В течение всех последующих измерений не изменяйте настройки уровня источника тестового акустического сигнала и не регулируйте уровень громкости на АС.

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2, в графу $V_{c1\,i}$, где i – номер октавной полосы (от 1 до 5).

4.5.2 Измерение уровня фонового виброшума

Для измерения уровня фонового виброшума в контрольной точке выполните следующие действия:

− закрепите измерительный вибродатчик в контрольной точке при помощи необходимых элементов крепления;

− установите АС на расстоянии 1,5 м от ОК/ИК;

− используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – накопление минимумов, количество циклов накопления – 30. Нажмите кнопку «Пуск». На панели анализатора спектра будут отображаться минимальные значения спектральных составляющих фоновой обстановки. Измерения необходимо проводить при минимальных уровнях внешних шумов (при отсутствии персонала, при выключенных системах кондиционирования и вентиляции и пр.). Через 30 сек, после того, как загорится зеленый индикатор справа от элемента «Количество циклов накопления», нажмите кнопку «Стоп».

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2, в графу $V_{\text{ш}\,i}$, где i – номер октавной полосы (от 1 до 5).

4.5.3. Измерение уровня вибросигнала в контрольной точке

На панели управления модулем акустического сигнала с помощью элемента «Выход» установите «Белый шум». Запустите сбор информации, нажатием кнопки «Пуск» на панели управлении измерительным модулем. Через 30 сек нажмите кнопку «Стоп». Отключите генерацию шума (в окне управления модулем акустического сигнала установите режим «Выход» – «Блокировка»).

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 4.2 в графу $V_{(\text{с+ш})\,i}$, где i – номер октавной полосы (от 1 до 5).

Примечание: если выбранная контрольная точка находится на одном из внутренних стекол оконного проема, то очевидно, что ввиду большой жесткости стекла измерения тестового вибросигнала (п. 4.5.1) и вибросигнала в данной контрольной точке дадут практически одинаковый результат (разница будет небольшой из-за того, что при оценке тестового сигнала акустическая система располагается на расстоянии 1 м от ОК/ИК, а при измерении вибросигнала в контрольной точке требуется располагать АС на расстоянии 1,5 м от поверхности ИК/ОК). Поэтому понятно без всяких измерений, что коэффициент виброизоляции в данном случае будет стремиться к нулю, если не применяются средства активной защиты.

4.5.4. Расчет коэффициентов виброизоляции

Рассчитайте октавные уровни виброакустического сигнала $V_{\text{с}2i}$ по формулам (1):

$$V_{\text{с}2i} = \begin{cases} V_{(\text{с+ш})_i} & \text{при} \quad V_{(\text{с+ш})_i} - V_{\text{ш}_i} \geq 10 \\ V_{(\text{с+ш})_i} - \Delta & \text{при} \quad V_{(\text{с+ш})_i} - V_{\text{ш}_i} < 10 \end{cases}, \qquad (1)$$

где Δ – поправка в дБ, определяемая из табл. 4.1.

Таблица 4.1

$V_{(с+ш)\,i}$	> 10	6…10	4…6	3	2	1	0,5
Δ, дБ	0	1	2	3	4	7	10

Запишите рассчитанные значения V_{c2i} в табл. 4.2.

Октавные уровни виброизоляции G_i рассчитываются по формуле (2):

$$G_i = V_{\text{с}1_i} - V_{\text{с}2_i} \qquad (2)$$

Запишите рассчитанные значения G_i в табл. 4.2.

Сравните полученные значения G_i с требуемыми нормативными значениями, приведенными в табл. 4.3. Если хотя бы один из коэффициентов виброизоляции меньше, чем нормированное значение, делается вывод о недостаточности виброизоляции и следовательно о незащищенности помещения от утечки речевой информации.

Таблица 4.2

Результаты расчетов октавных коэффициентов виброизоляции

Номер октавной полосы, i	Измеренный уровень виброакустического шума в контрольной точке $V_{ш\,i}$, дБ	Уровень тестового сигнала $V_{с1i}$, дБ	Уровень измеренного суммарного виброакустического сигнала и виброакустического шума в контрольной точке $V_{(с+ш)\,i}$, дБ	Расчетный уровень виброакустического сигнала в контрольной точке V_{c2i}, дБ	Октавные уровни виброизоляции в контрольной точке G_i, дБ
Контрольная точка №					
1					
2					
3					
4					
5					

Таблица 4.3

Нормативные значения коэффициента звукоизоляции

Место возможного перехвата речевой конфиденциальной информации из помещения		Нормативное значение октавного коэффициента звукоизоляции, дБ	
		для помещений, не оборудованных системами звукоусиления	для помещений, оборудованных системами звукоусиления
Смежные помещения		46	60
Уличное пространство	Улица без транспорта	36	50
	Улица с транспортом	26	40

4.6. Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

- завершите работу с программой;
- выключите АС выключателем питания;
- выключите модуль тестового акустического сигнала;
- выключите измерительный модуль;
- отсоедините измерительный вибродатчик, упакуйте его в предназначенную коробку.
- отключите модуль сопряжения;
- сложите все компоненты комплекса в сумку.

5. Содержание отчета

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации (рекомендуемая форма протокола приведена в приложении Б), а также ответы на контрольные вопросы.

6. Контрольные вопросы

6.1. Какими особенностями характеризуются распространение звуковых колебаний в инженерных конструкциях?

6.2. Каким образом осуществляется съем речевой информации по виброакустическому каналу?

6.3. Зависит ли спектральный состав виброшума в контрольной точке от механической жесткости проверяемой ОК?

6.4. Назовите наиболее известные генераторы акустического и виброакустического маскирующего шума.

6.5. Цель проведения технического контроля акустической защищенности выделенного помещения.

6.6. Относительно каких мест проводится технический контроль акустической защищенности выделенного помещения?

6.7. Что предполагает инструментальный контроль акустической защищенности выделенных помещений?

6.8. Какой сигнал необходимо использовать в качестве тестового при виброакустическом инструментальном контроле?

6.9. Требования к выбору контрольных точек для вибрационных измерений при проверке выполнения норм противодействия акустической речевой разведке, если через границу контролируемой зоны проходят коммуникации инженерно-технических систем.

6.10. На чем базируется действующая методика измерений акустических и виброакустических характеристик различных сред?

6.11. Как определяется реальное затухание сигнала в виброакустическом канале утечки речевой информации?

Приложение А

Крепежные элементы вибродатчика

Рис. 1П. Хомут для крепления вибродатчика на трубы отопления и водоснабжения

Рис. 2П. Площадка для крепления вибродатчика на стекла и гладкие поверхности

Рис. 3П. Шпилька для крепления вибродатчика на стены

Примеры крепления вибродатчика

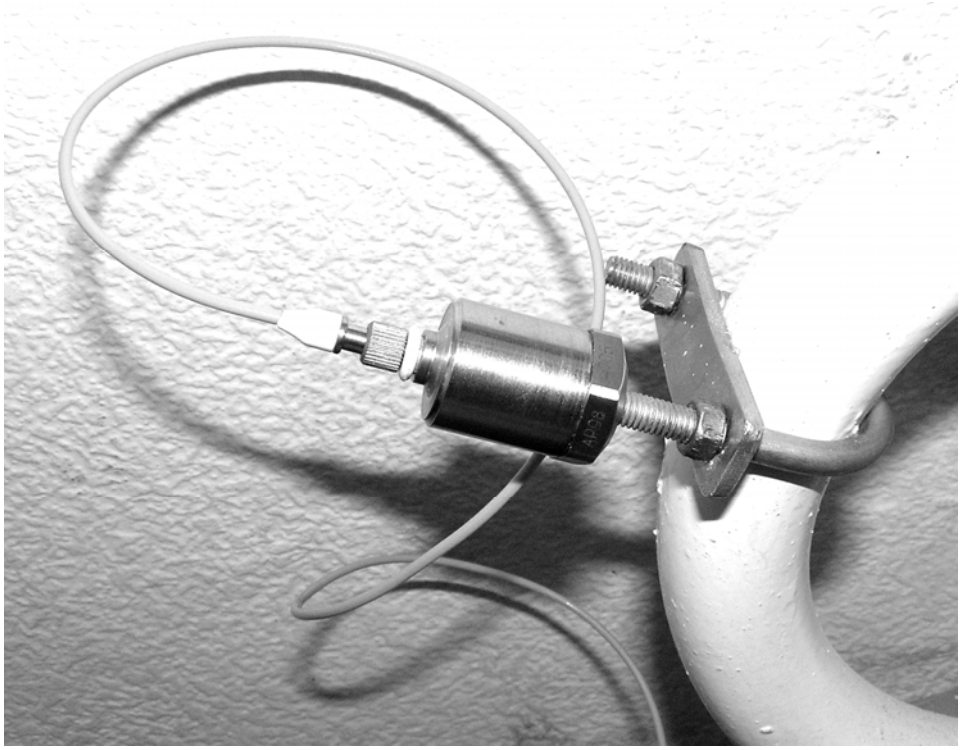


Рис. 4П. Крепление вибродатчика на батарею отопления

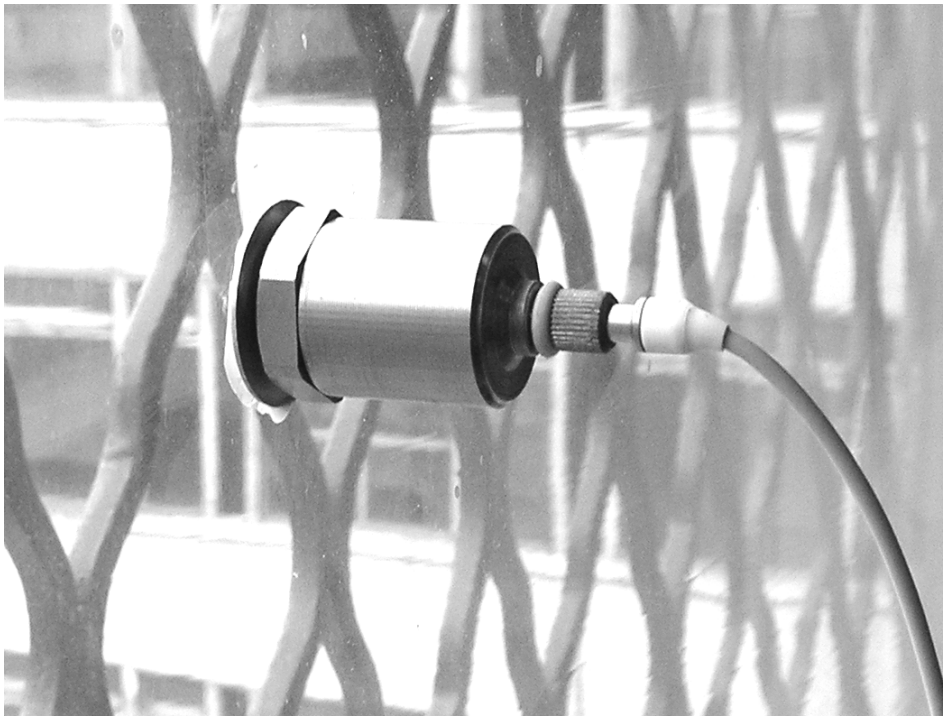


Рис. 5П. Крепление вибродатчика на стекло

Приложение Б

Рекомендуемая форма протокола инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации

ПРОТОКОЛ
инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации

1. Объект оценки (наименование помещения, адрес).

2. Назначение помещения и его краткое описание (расположение помещения, план-схема помещения).

3. Вид оценки – аттестационный контроль.

4. Вид оцениваемого канала перехвата речевой информации – виброакустический (оптико-электронный).

5. Оцениваемые ограждающие конструкции и элементы технических систем (окно, дверь, стены, пол, потолок, вент. канал и т.д.).

6. Описание применяемых мер и средств защиты (уплотненные притворы дверей, шторы, организационные меры и т.п.).

7. Перечень средств измерений и вспомогательного оборудования (наименование, тип, заводской номер, дата очередной поверки).

8. Перечень нормативных и методических документов, используемых при оценке защищенности.

(Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, Гостехкомиссия России, 2002).

9. Результаты измерений и расчетов виброизоляции.

10. Заключение о выполнении требований по защите (выполняются, не выполняются).

Оценку защищенности выполнил

_____ _____

(наименование должности, инициалы, фамилия) (личная подпись)

Дата

Лабораторная работа №7

ОЦЕНКА ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ С ПОМОЩЬЮ КОМПЛЕКСА «СПРУТ-7»

1. Цель работы

Изучить методику применения комплекса Спрут-7 при оценке защищенности помещения от утечки речевой информации по каналам акустоэлектрических преобразований в технических средствах. Научиться оценивать октавные соотношения «сигнал/шум» и оформлять результаты измерений.

2. Краткие теоретические сведения

Практически в любом помещении находятся те или иные технические средства (ТС): это телефон, различные пожарные и охранные датчики, оргтехника, системы связи и т.д. И эти технические средства в нормальном режиме работы могут образовывать каналы утечки информации.

Достаточно хорошо известны способы несанкционированного получения информации об акустике помещения за счет подсоединения к линиям телефонных аппаратов (особенно аппаратов с электромеханическими звонками), линиям диспетчерской или громкоговорящей связи, вторичной часофикации, некоторым линиям охранной сигнализации и даже линиям электропитания. Подобные каналы утечки создаются за счет явления акустоэлектрических преобразований (АЭП) в элементах ТС.

Акустоэлектрический преобразователь – это устройство, преобразующее акустическую энергию (т.е. энергию упругих волн в воздушной среде) в электромагнитную энергию в схемах тех устройств, в которых находятся акустоэлектрические преобразователи. Наиболее распространенные акустоэлектрические преобразователи линейны, т.е. удовлетворяют требованиям неискаженной передачи сигнала, и обратимы, т.е. могут работать и как излучатель и как приемник (подчиняются принципу взаимности).

В основе явления АЭП лежат следующие физические эффекты:

− электродинамический эффект – возникновение ЭДС (тока) в обмотке, колеблющейся в магнитном поле;

− электромагнитный эффект – изменение магнитного потока через ферромагнитный сердечник при его механическом перемещении, вызванном акустическими колебаниями и, следовательно, изменение тока в его обмотке;

− электростатический эффект – изменение расстояния между обкладками конденсатора (например, воздушного) и следовательно изменение напряжения на нем;

− обратный эффект магнитострикции (эффект Веллари) – преобразование механической энергии, прикладываемой к сердечнику из магнитострикционного материала, в энергию магнитного поля, вызывающую ЭДС в обмотке. Такие конструкции используются в фильтрах, резонаторах и т.п.;

− пьезоэлектрический эффект – возникновение напряжения на поверхностях некоторых кристаллический веществ при их сжатии и растяжении;

− тензорезистивный эффект – изменение сопротивления полупроводниковых приборов при приложении к ним механических усилий.

Проявление акустопреобразовательных каналов утечки информации в большинстве случаев не связано с качеством исполнения того или иного технического средства, а является сопутствующим его деятельности. В ряде случаев они возникают за счет взаимности действия элемента, заложенного в конструкцию (динамики), в других случаях за счет некачественного исполнения элементов (рыхлая намотка индуктивностей, изменение расстояния между обкладками конденсатора и т.п.).

Таким образом, как следует из перечисления возможных механизмов преобразования, значительное количество элементов окружающих нас различных устройств, может обладать акустопреобразовательным эффектом, и следовательно, может являться источником для создания канала утечки конфиденциальной акустической информации.

В данной работе применяется методика инструментально-расчетной оценки возможности утечки речевой конфиденциальной информации по каналам электроакустических преобразований, разработанная Гостехкомиссией России. Методика подразумевает оценку только прямых акустоэлектрических преобразований, т.е. тех, сигналы которых распространяются по проводам и частотный диапазон которых находится в частотном диапазоне речевого сигнала.

Метод оценки заключается в инструментально-расчетном определении совокупности октавных отношений напряжений, наводимых в функциональных (сигнальных) цепях ТС тестовым акустическим сигналом и шумом за счет их акустоэлектрических преобразований и последующим сравнением этих отношений с нормативными значениями.

3. Применяемое оборудование

Для измерений сигналов АЭП, как правило, имеющих крайне малые величины, в состав комплекса «Спрут-7» входят специальные дифференциальные усилители, выполненные в виде отдельных устройств. Каждый усилитель имеет внутренние аккумуляторы, фиксированные коэффициенты усиления 20, 40, 60 дБ. Кроме того, усилитель №2 имеет встроенный режекторный фильтр на частоту 50 Гц для уменьшения влияния наводок сети электропитания на результат измерений. Усилители позволяют измерять сигналы на симметричных и несимметричных проводных линиях. Если один из входов усилителя не используется, он закорачивается специаль-

ной заглушкой. В общем случае проводные линии необходимо исследовать в обоих режимах. Все измерения проводятся при отключенном питании исследуемого технического средства и при отсутствии напряжений на отходящих линиях. Исключение составляют телефоны и некоторые датчики пожарной сигнализации, при исследовании которых на них подается питание.

Внешний вид дифференциального усилителя приведен на рис. 1, внешний вид передней панели усилителя №1 приведен на рис. 2.

Рис. 1. Внешний вид дифференциального усилителя №1

Рис. 2. Внешний вид передней панели дифференциального силителя №1

На передней панели дифференциального усилителя расположен выключатель питания, а также прямой и инверсный входы усилителя. На задней панели усилителя расположен выходной разъем, через который усилитель подключается к измерительному модулю прилагаемым к комплексу

кабелем, разъем для подключения зарядного устройства и переключатель коэффициента усиления.

Для питания телефонов, датчиков пожарной сигнализации и некоторых других технических средств в состав комплекса входит источник питания «SZPS-01» (рис. 3).

Рис. 3. Внешний вид источника питания

Кроме питания ТС, источник питания «SZPS-01» предназначен для зарядки измерительных усилителей. Подключение ТС к источнику питания осуществляется через специальный переходник (рис. 4). К переходнику может непосредственно подключаться исследуемый телефонный аппарат, кроме того, на переходнике имеется разъем для непосредственного подключения дифференциального усилителя.

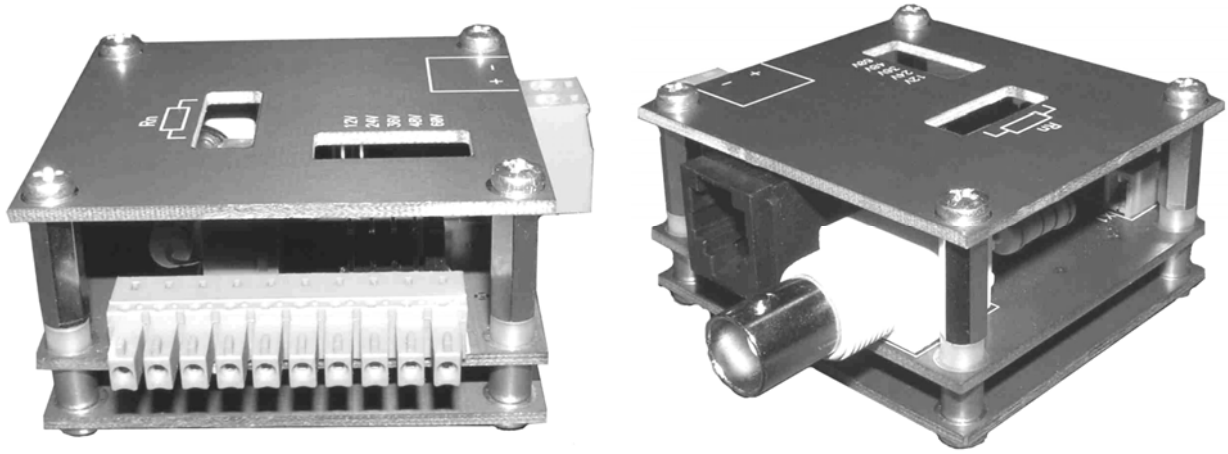


Рис. 4. Внешний вид переходника для подключения питания на технические средства

4. Задание на выполнение работы

4.1. Изучить особенности заданного технического средства, предварительно оценить возможность возникновения АЭП.

4.2. Подготовить комплекс «Спрут-7» для проведения измерений АЭП.

4.3. Провести измерения сигналов АЭП.

4.4. Оформить протокол оценки защищенности помещения.

4.5. Ответить на контрольные вопросы.

5. Порядок выполнения работы

5.1. Составьте план-схему размещения ТС в помещении, отметьте линии, выходящие за пределы помещения.

5.2. Подготовьте комплекс «Спрут-7» для проведения акустических измерений. Для этого:

− подключите модуль сопряжения к ПЭВМ;

− подключите измерительный микрофон к измерительному модулю. Подключите антенну к измерительному модулю. Включите питание измерительного модуля;

− подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сигнала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.

− запустите программное обеспечение для управления комплексом. Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:

− тип входного датчика – микрофон;

− кнопка «Полный спектр» отжата;

− чувствительность – низкая;

− фильтры 1/1 октавы;

− панель источника тестового сигнала – активна;

− уровень выходного сигнала источника тестового акустического сигнала – минимум;

− тип выхода – блокировка.

5.3. Измерение октавных уровней тестового акустического сигнала

В качестве тестового акустического сигнала при измерении уровней АЭП необходимо использовать гармонические тональные сигналы с определенными уровнями. Поэтому необходимо «откалибровать» комплекс «Спрут-7».

5.3.1. Разместите микрофон на расстоянии 1 м от АС. Используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 – текущий спектр.

5.3.2. На панели управления модулем акустического сигнала с помощью элемента «Синус» установите частоту выходного сигнала в соответствии с табл. 5.1, в элементе управления «Выход» установите «Синус».

5.3.3. Нажмите кнопку «Пуск». С помощью регулятора уровня в панели источника тестового акустического сигнала начинайте увеличивать громкость воспроизводимого тонального сигнала. Добейтесь октавного уровня сигнала, указанного в табл. 5.1. Измерения уровня производите

курсором в окне анализатора спектра по центру соответствующей октавной полосы (не спутайте октавный уровень сигнала с интегральным).

5.3.4. Запишите значение регулятора уровня панели источника акустического сигнала в табл. 5.1.

5.3.5. Повторите п. 5.3.2, п. 5.3.3, п. 5.3.4 для каждого значения частоты, указанной в табл. 4.1.

Таблица 5.1

Октавные уровни тестовых сигналов

Среднегеометрическая частота октавной полосы, Гц	Требуемый октавный уровень тестового сигнала, дБ	Значение уровня громкости в панели источника акустического сигнала
250	66	
500	66	
1000	61	
2000	56	
4000	53	

5.3.6. Завершите измерения уровней тестового акустического сигнала. Выключите измерительный модуль, отключите и упакуйте измерительный микрофон.

5.4. Измерение уровня октавного шума

5.4.1. Подключите ко входу измерительного модуля дифференциальный усилитель №1,2. Входы усилителя при помощи прилагаемых осциллографических пробников подключите к исследуемой линии по симметричной (рис. 1) или несимметричной схеме (рис. 2)

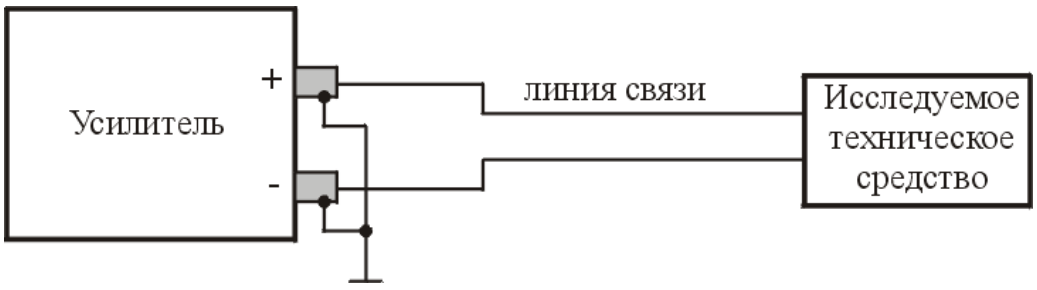


Рис. 1. Симметричная схема подключения

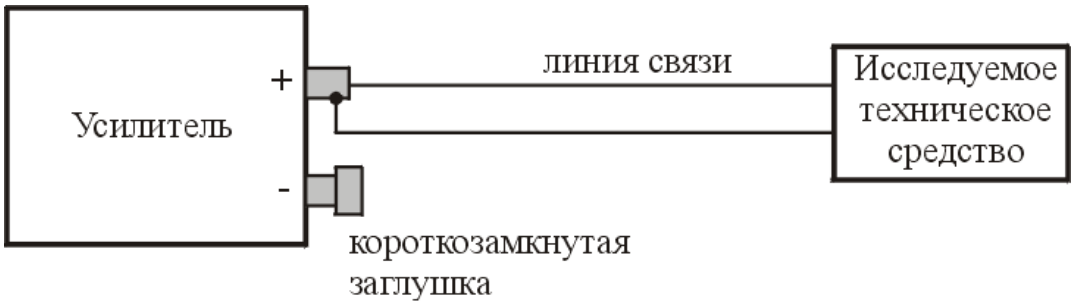


Рис. 2. Несимметричная схема подключения

5.4.2. Если исследованию подвергается ТС, требующее подачи питания (телефон, датчики пожарной сигнализации и т.п.), подключите питание ТС от источника питания «SZPS-01». К разъему переходника (рисунок 3.4) подключите один из входов дифференциального усилителя (в этом случае возможно только несимметричное подключение).

5.4.3. Включите дифференциальный усилитель.

5.4.4. Включите измерительный модуль.

5.4.5. Проведите настройку программного обеспечения (на панели датчиков):

– тип входного датчика – прямой вход;

– усилитель №1,2 (20 дБ, 40 дБ или 60 дБ) в зависимости от положения переключателя на задней панели усилителя.

5.4.6. На панели управления измерительным модулем включите режим графика №1 – текущий спектр. Нажмите кнопку «Пуск». В окне анализатора спектра должен отобразиться текущий спектральный состав напряжения шумов, присутствующих на входном разъеме дифференциального усилителя.

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 5.2, в графу $U_{\text{ш.окт }i}$, где i – номер октавной полосы (от 1 до 5).

5.5. Измерение уровней сигналов акустоэлектрических преобразований (АЭП)

5.5.1. Расположите АС на расстоянии 1 метр от исследуемого ТС. В панели управления модулем акустического сигнала с помощью элемента «Синус» установите частоту выходного сигнала в соответствии с табл. 5.1, в элементе управления «Выход» установите «Синус». Уровень выходного сигнала для заданной выходной частоты установите на значение, соответствующее заданной частоте (табл. 5.1).

5.5.2. В окне анализатора спектра необходимо зафиксировать превышение уровня сигнала в i-й октавной полосе над уровнем шума ($U_{\text{ш.окт }i}$). Если изменений нет или они слишком малы, попытайтесь увеличить коэффициент усиления дифференциального усилителя (20 дБ, 40 дБ), либо используйте другой усилитель (40 дБ, 60 дБ), а также изменить чувствительность измерительного модуля (элемент управления «Чувствительность»). Запишите уровень измеренного сигнала в заданной полосе в табл. 5.2.

5.5.3. Изменяя частоту и уровень выходного сигнала в соответствии с табл. 5.1, измерьте уровни сигналов в соответствующей октавной полосе и запишите их в табл. 5.2.

5.5.4. Измерения по п.5.5.1–5.5.3 необходимо провести для случаев симметричного и несимметричного подключения, а также для всех возможных режимов работы ТС, для каждого режима заполняя новую табл. 5.2. Например: при исследовании сигналов АЭП бытового вентилятора не-

обходимо произвести измерения при всех возможных положениях переключателя скоростей и т.д.

5.6. Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

- завершите работу с программой;
- выключите АС выключателем питания;
- выключите модуль тестового акустического сигнала;
- выключите измерительный модуль;
- выключите дифференциальный усилитель;
- отключите модуль сопряжения;
- сложите все компоненты комплекса в сумку.

5.7. Выполнение расчетов

Результаты измерений заносятся в табл. 5.2. Значения в графах «Уровень шума в линии связи, $U_{\text{ш.окт}\,i}$, мкВ» и «Уровень сигнала АЭП в линии связи $U_{\text{с}\,i}$, мкВ» рассчитываются по формуле 1.

$$U(\text{мкв}) = 10^{\frac{U(\text{дБ})}{20}}. \qquad (1)$$

Расчет отношения «сигнал/шум» в каждой октавной полосе производится по формуле 2.

$$\Delta i = \frac{U_{\text{с}\,i}}{U_{\text{ш окт}\,i}}. \qquad (2)$$

Таблица 5.2

Результаты измерений

Среднегеометрическая частота октавной полосы, Гц	Уровень шума в линии связи $U_{\text{ш.окт}\,i}$, дБ	Уровень шума в линии связи $U_{\text{ш.окт}\,i}$, мкВ	Уровень сигнала АЭП в линии связи $U_{\text{с}\,i}$, дБ	Уровень сигнала АЭП в линии связи $U_{\text{с}\,i}$, мкВ
250				
500				
1000				
2000				
4000				

Нормативное значение отношения «сигнал/шум» = 0,3, т.е. информация считается защищенной, если $\Delta i < 0{,}3$.

6. Содержание отчета

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации (рекомендуемая форма протокола приведена в приложении), а также ответы на контрольные вопросы.

7. Контрольные вопросы

7.1. В чем заключается эффект акустоэлектрических преобразований?

7.2. Какие физические эффекты лежат в основе АЭП предложенного Вам в лабораторной работе технического средства?

7.3. Какие устройства с акустоэлектрическим эффектом могут входить в состав некоторых ВТСС?

7.4. В чем заключается эффект модуляционного акустоэлектрического преобразования?

7.5. В каком случае проводную линию следует рассматривать как несимметричную?

7.6. Назовите наиболее простой способ выявления факта модуляции сигнала модуляционного акустоэлектрического преобразователя.

7.7. По какому признаку делается вывод о наличии акустоэлектрических преобразований ВТСС?

7.8. Если акустоэлектрические преобразования обнаружены, то каким образом можно оценить их опасность?

7.9. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.

7.10. Каким образом осуществляется перехват речевого сигнала в акустоэлектрическом канале?

Приложение

Рекомендуемая форма протокола оценки защищенности помещения от утечки речевой конфиденциальной информации по каналам акустоэлектрических преобразований

ПРОТОКОЛ
оценки защищенности помещения
от утечки речевой конфиденциальной информации
по каналам акустоэлектрических преобразований

1. Место расположение защищаемого помещения _____

_____

2. План-схема помещения с размещением в нем ТС (оформляется отдельным листом)

3. Перечень потенциально опасных ТС (т.е. ТС, имеющих выход за пределы помещения)

Наименование ТС	Тип (модель) ТС	Заводской номер	Примечание

4. Перечень средств измерений и вспомогательного оборудования

Наименование средств измерений и вспомогательного оборудования	Тип	Заводской номер	Дата очередной поверки

5. Результаты измерений и расчетов

Наименование и заводской номер ТС	Режим работы	Выходной разъем цепи	$U_{ш.окт\,i}$, мкВ, на среднегеометрических частотах (250, 500, 1000, 2000, 4000) октавных полос					$U_{с\,i}$, мкВ, на среднегеометрических частотах (250, 500, 1000, 2000, 4000) октавных полос				

Наименование и заводской номер ТС	Режим работы	Выходной разъем цепи	Δi на среднегеометрических частотах (250, 500, 1000, 2000, 4000) октавных полос					Соответствие нормативному значению на среднегеометрических частотах (250, 500, 1000, 2000, 4000) октавных полос				

6. Выводы о защищенности помещения:

_____

_____

_____

_____

_____ _____

(наименование должности, инициалы, фамилия) (личная подпись)

Дата

Лабораторная работа №8

ОБНАРУЖЕНИЕ ПЭМИ ПО ЭЛЕКТРИЧЕСКОЙ СОСТАВЛЯЮЩЕЙ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ С ПОМОЩЬЮ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «ЛЕГЕНДА»

1. Цель работы

Изучение порядка проведения поиска и измерения ПЭМИ по электрической составляющей и расчет параметров защищенности технических средств от утечки информации.

2. Теоретические сведения, необходимые для проведения специсследований

Исследование побочного электромагнитного излучения монитора необходимо проводить с помощью измерительных антенн «Альбатрос».

Проблема выделения сигналов, обладающих информационными признаками и относящихся к излучению исследуемого устройства, может быть решена с использованием:

– энергетического принципа пропадания сигнала при отключении контролируемого устройства;

– информационного принципа, когда перед проведением исследования производится формирование эталонного образа искомого сигнала, и в процессе исследования осуществляется автоматическое обнаружение сигналов в эфире, похожих на этот эталонный сигнал.

Сравнение обнаруженного сигнала и образа эталонного сигнала производится путем вычисления максимума взаимнокорреляционной функции между образами сигналов. При превышении данной величиной установленного порогового значения, принимается решение о схожести образов. При этом исключается возможность причисления к перечню обнаруженных частот посторонних сигналов и неинформативных ПЭМИ исследуемого технического средства.

Работа в управляющей программе сводится к поиску эталона тестового сигнала в полуавтоматическом режиме, составлению программ исследований для предварительного контроля электромагнитной обстановки (ЭМО) и автоматического поиска по заданному эталону похожих сигналов.

3. Задание для проведения работы

3.1. Изучить методику проведения специсследования.

3.2. Провести поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы.

3.3. Составить протокол исследования с помощью расчетной программы.

3.4. Сделать выводы.

4. Порядок выполнения работы

4.1. Подготовка комплекса и исследуемого средства к работе

4.1.1. Управляющую ПЭВМ и измерительный прибор необходимо соединить кабелем USB.

4.1.2. Подключить антенну «нулевая диполь» (А117.3) к анализатору спектра R&S FS300 с помощью кабеля А117.3 к разъему (8).

4.1.3. Включить анализатор спектра.

4.1.4. Включить на исследуемом техническом средстве монитор тест «Зебра».

4.1.5. Запустить управляющую программу на персональном компьютере.

4.2. Поиск и измерение ПЭМИ в автоматическом режиме измерений

4.2.1. Создание эталона тестового сигнала

Для перехода в полуавтоматический режим измерений выберите в меню главного окна программы пункт «Измерения – Ручной режим» или нажмите соответствующую кнопку быстрого запуска. На экране управляющей ПЭВМ выводится окно полуавтоматического режима, показанное на рис. 1.

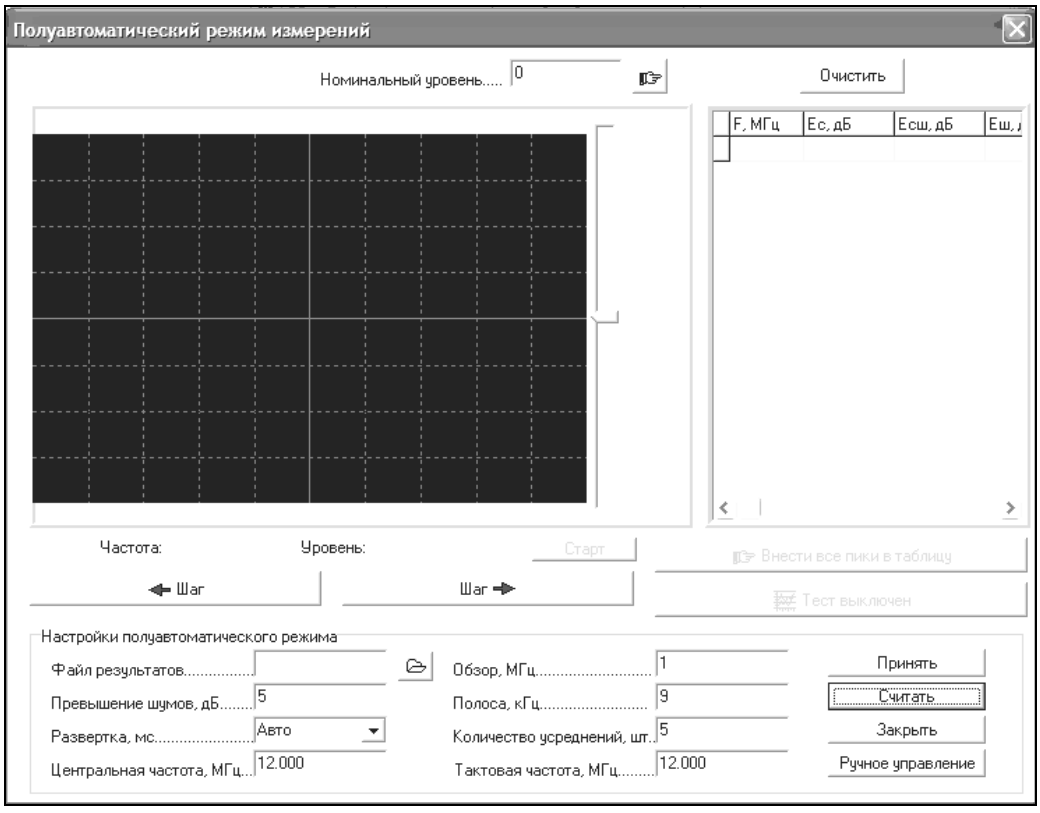


Рис. 1. Окно полуавтоматического режима

В предыдущей лабораторной работе в ручном режиме с помощью анализатора спектра вы нашли примерно ожидаемую тактовую частоту теста монитора. Это значение необходимо ввести в поле «Центральная частота», обзор установите равным 4МГц, остальные поля заполните согласно реко-

мендациям, приведенным в предыдущей лабораторной работе. Нажмите кнопку «Принять». На дисплее окна полуавтоматического режима изображается текущее усреднение трека спектра. По завершении усреднений картинка останавливается.

Выключите тест на мониторе и нажмите «Тест выключен». На дисплее окна полуавтоматического режима отображаются в одной системе координат два графика частотного спектра (рис. 2): синим цветом с заполнением отображается график спектра при выключенном тесте, зеленым цветом – график спектра при включенном тесте. Белым цветом с заполнением показывается превышение шумов. Все видимые пики «зеленого» графика подлежат анализу как «подозрительные».

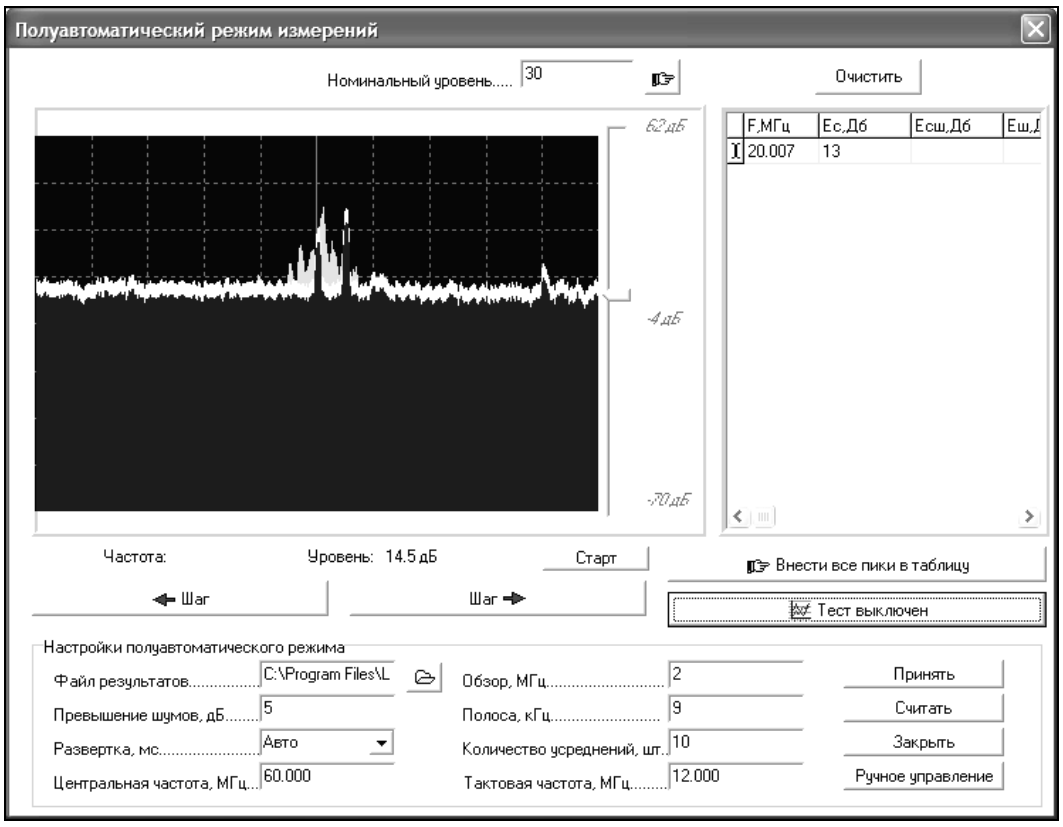


Рис. 2. Графики частотного спектра

Исследуйте все видимые пики «зеленого» графика. Для этого подведите курсор «мыши» к выбранному пику, удерживая нажатой левую кнопку «мыши». При этом внизу под дисплеем отображается значение частоты, совместно с курсором «мыши» перемещается маркер желтого цвета. Настроившись на нужный пик, отпустите левую кнопку «мыши». Поверх окна полуавтоматического режима выводится окно просмотра пика (рис. 3).

Включая и выключая тестовый режим работы исследуемого технического средства и наблюдая за осциллограммой, установите, принадлежит ли данное излучение гармоническим составляющим тестового сигнала. При обнаружении тестового сигнала следует сохранить его как эталон, на-

жав на кнопку «Сохранить как эталон» окна просмотра пика. Сохраните в созданную папку со своим номером группы.

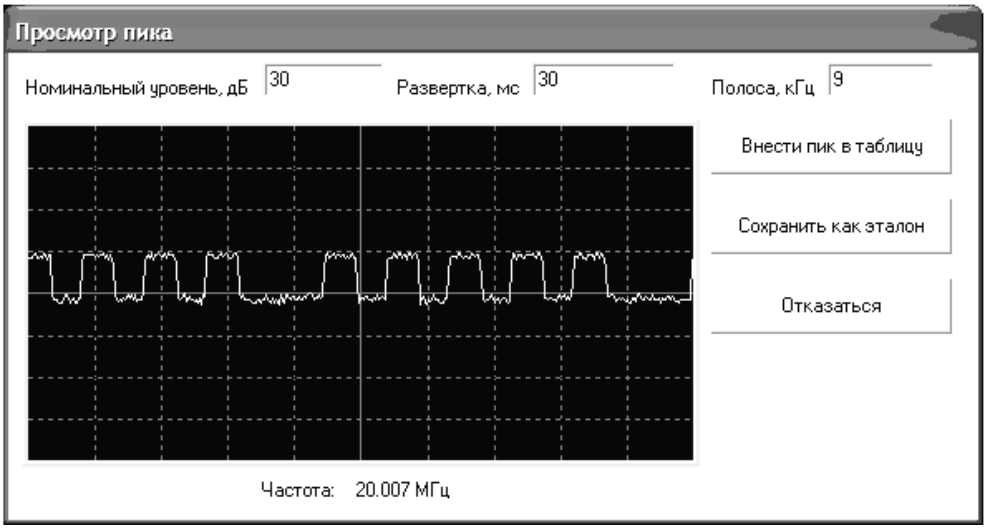


Рис. 3. Осциллограмма сигнала, демодулированного при помощи измерительного прибора

4.2.2. Контроль электромагнитной обстановки (ЭМО)

4.2.2.1. Выключите тест на исследуемом средстве;

4.2.2.2. Для предварительного контроля ЭМО следует составить программу исследования, для этого выберите в меню главного окна программы «Установки/Программа исследований». Поверх главного окна программы откроется окно параметров исследования на странице программы исследований (рис. 4).

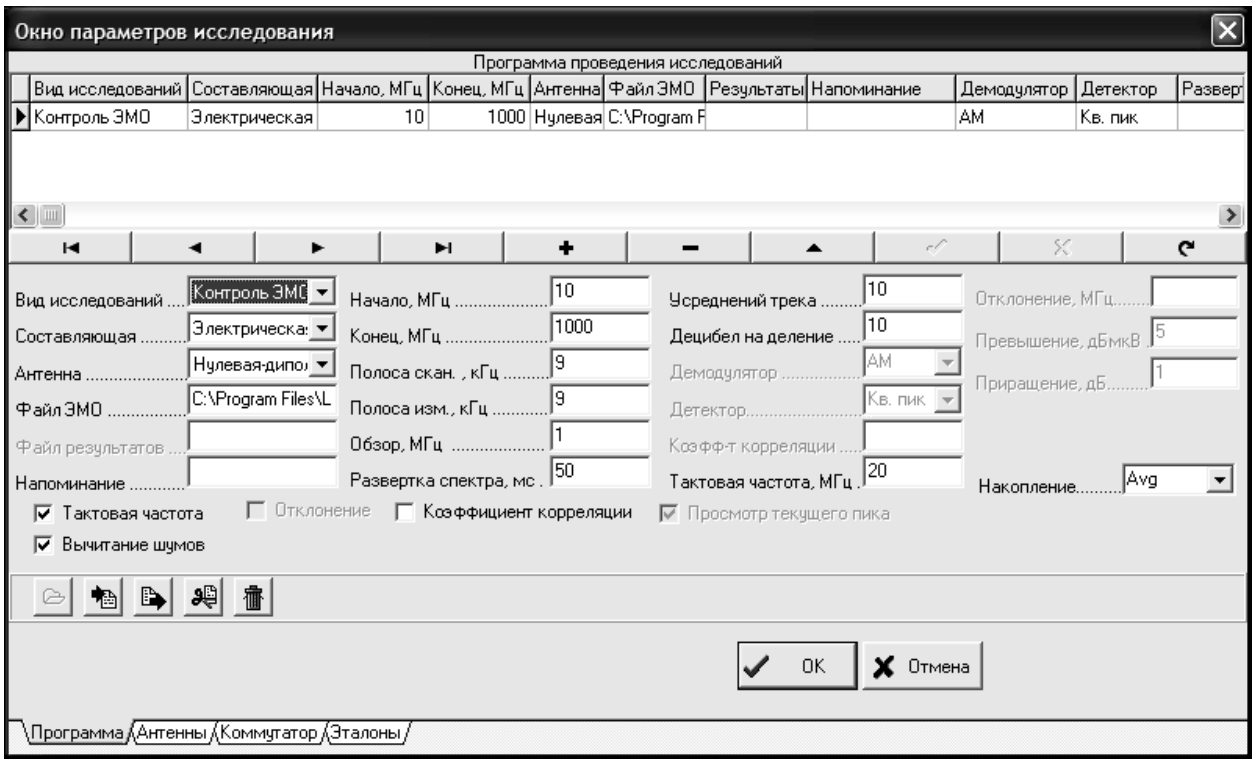


Рис. 4 . Окно параметров исследования

4.2.2.3. В таблице программы исследования, расположенной в верхней части страницы, отображается готовая к исполнению программа. По умолчанию таблица содержит программу, составленную при прошлом запуске управляющей программы. Сотрите старую программу нажатием кнопки «Мусорная корзина». Для экономии времени проведите контроль в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц (для монитора на ЖК).

4.2.2.4. После заполнения программы, внесите ее в таблицу нажатием кнопки «Внести в таблицу».

4.2.2.5. Нажмите кнопку «Ок». Программа автоматически сканирует выбранный диапазон и по завершении выдает сообщение «Программа исследования завершена». При этом, результаты сканирования сохранены в соответствующих выбранных файлах ЭМО для каждого диапазона и их можно использовать для автоматического поиска составляющих тестового сигнала при включенном тесте.

4.2.3. Автоматический поиск составляющих тестового сигнала

Автоматический поиск гармонических составляющих тестового сигнала по заданному эталону можно производить методом беспропускового контроля по всему диапазону проведения специсследования, либо в окрестностях частот, кратных тактовой частоте теста. Для экономии времени проведите исследование в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц (для монитора на ЖК).

4.2.3.1. Для поиска составляющих тестового сигнала следует заполнить программу исследований. Для этого достаточно заменить вид исследований во всех заполненных строках таблицы на «Измерение ПЭМИН»;

4.2.3.2. После заполнения программы исследования загрузите эталон, найденный в полуавтоматическом режиме. Примерный вид эталона представлен на рис. 5.

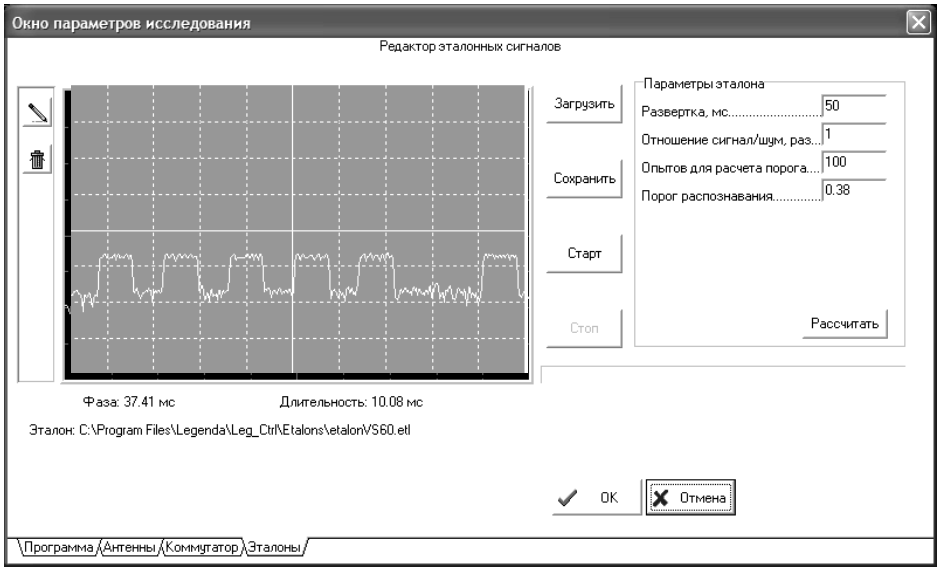


Рис. 5. Эталон тестового сигнала монитора на ЭЛТ

4.2.3.3. Рассчитайте пороговый коэффициент корреляции, нажав на кнопку «Рассчитать», после чего появится следующее окно (рис. 6).

4.2.3.4. Выберите в меню главного окна программы пункт «Измерения-Старт», либо нажмите соответствующую кнопку быстрого запуска. Программа начнет сканировать диапазон, выделять пики, превышающие на заданное значение уровень шумов при выключенном тесте (если используется файл ЭМО). Демодулированный сигнал будет сравниваться с эталоном и при превышении коэффициентом корреляции заданного порога, значение частоты будет занесено в таблицу. По завершении сканирования выдается сообщение «Выключите тест для измерения уровней шумов» и программа выполнит необходимые действия. В конце работы выдается сообщение «Программа исследований выполнена».

По завершении автоматического поиска и/или измерения ПЭМИН можно проконтролировать правильность обнаружения. Для этого щелкните «мышью» по любой строке таблицы обнаруженных частот главного окна управляющей программы. На основном дисплее главного окна программы будет отображаться в реальном времени осциллограмма демодулированного сигнала на данной частоте. Включая и выключая тест на исследуемом техническом средстве и наблюдая за изменениями формы осциллограммы, можно сделать вывод о принадлежности данного излучения к составляющим тестового сигнала. В случае ложного срабатывания процедуры распознавания строку с ошибочно распознанным сигналом можно удалить, для чего следует нажать CTRL-DEL на клавиатуре управляющей ПЭВМ.

Рис. 6. Расчет порогового коэффициента корреляции

4.3. Расчет зон разведдоступности с помощью расчетной программы

4.3.1. Для запуска расчетной программы следует выбрать в меню «Пуск» соответствующий ярлык или вызвать исполняемый файл, на который ссылается данный ярлык («Легенда»).

4.3.2. Для того, чтобы загрузить данные измерений из файла в расчетную программу нужно выбрать в меню «Файл» пункт «Открыть». Появится стандартный диалог открытия файлов Windows. Далее пользователь должен указать файл, в котором содержатся данные измерений для расчета, полученные при работе управляющей программы, и нажать кнопку «Открыть». В случае правильной структуры файла в поля рабочей таблицы «*F*, МГц», «*U*, дБ» и «$U_{ш}$, дБ» загрузятся значения частоты, уровня обнаруженных компонент тестового сигнала и уровня шума.

4.3.3. Для заполнения условий расчета следует выбрать в меню «Условия» команду «Заполнить». Пользуясь описанием процесса задания условий для расчета из предыдущей лабораторной работы, заполните условия, выставив отношение сигнал/шум для всех трех категорий 0,4.

4.3.4. После внесения и заполнения условий, нажмите Измерения-Старт. Программа рассчитает зоны разведдоступности.

4.3.5. После того, как программа выполнит расчет измерения, нужно сохранить результат в Microsoft Word с помощью кнопки быстрого доступа (документ Microsoft Word должен быть открыт).

5. Требования к отчету

Оформить отчет о проделанной работе. В отчете привести цель работы, задание на выполнение работы, порядок проведения работы, протоколы исследований в автоматическом и полуавтоматическом режимах. Сравнить результаты. Сделать выводы и ответить на контрольные вопросы.

6. Контрольные вопросы

6.1. Как решается проблема выделения информационных излучений?

6.2. Для чего необходим эталон тестового сигнала?

6.3. Каким образом происходит сравнение обнаруженного сигнала и образа эталонного сигнала?

6.4. Зачем необходим контроль ЭМО?

6.5. В каких режимах управляющая программа позволяет производить измерение ПЭМИН?

ПРИЛОЖЕНИЕ 1

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ НЕКОТОРЫХ УСТРОЙСТВ

Технические характеристики монокуляра с направленным микрофоном «Супер Ухо-30»

1. Устройство «Супер Ухо-30» обеспечивает до 40 децибел окружающего звукового увеличения.
2. Высокочувствительный мульти-элемент микрофона собирает звуки для усиления на расстоянии до 30 метров
3. Максимальная мощность 107 дБ.
4. Диапазон частот 100–14000 герц.
5. Питание – две 1,5 м AAA щелочных батареи, которые обеспечивают до 80 часов работы устройства.
6. Вес 65 грамм (без упаковки и наушников). Размеры: 9,0×5,0×2,0 см
7. Температурный режим: от 0 °С до + 55 °С.
8. Максимальная влажность до 95% при температуре 20 °С.
9. Угол направленности 15°
10. Прибор работает только в пределах прямой видимости

Технические характеристики направленного микрофона «Yukon»

Звуковое усиление микрофона, дБ	0–66
Частотный диапазон микрофона, Гц	500–10000
Чувствительность микрофона по свободному полю на частоте 1000 Гц, мВ/Па	20±5
Уровень эквивалентного звукового давления, дБ	20
Габаритные размеры, мм	310×45×30
Масса микрофона, г	130
Источник/Напряжение питания	CR 123A/3B
Время непрерывной работы, час.	300

Технические характеристики прибора ночного видения с направленным микрофоном «nvs 2,5×42»

Визуальное увеличение, крат	2,5
Вертикальное разрешение, линий/мм	30
Угол поля зрения	15°
Максимальная дистанция наблюдения, м	200
Звуковое усиление микрофона прибор ночного видения с направленным микрофоном nvs 2,5×42	0–66 дБ
Диапазон частот	500–10000 Гц
Чувствительность микрофона по свободному полю на частоте 1000 Гц	20+5 мВ/Па
Дальность действия ИК-осветителя, м	90
Напряжение питания	3В (2АА)
Габариты, мм	310×95×70
Масса, кг	0,5
Размер резьбы крепления	1/4 дюйма
Время непрерывной работы	до 20 ч

Технические характеристики тепловизора «ThermaCAM P640»

Параметры визуализации

Поле зрения / минимальное расстояние фокусировки	24×18°/ 0,3 м
Оптическое разрешение (IFOV)	0,65 mrad
Температурная чувствительность	0,08 mK при 30 °C
Частота кадров	30 Гц без перемежения
Фокусировка	Ручная или автоматическая (объектив Ultrasonic)
Электронное увеличение/сдвиг	2, 4, 8 кратное / плавный
Тип детектора	Матрица в фокальной плоскости (FPA), неохлаждаемый микроболометр: 640×480 пикселей
Спектральный диапазон	От 7,5 до 13 мкм
Режимы обработки ИК изображения	Обычный или улучшенный
Встроенная цифровая видеокамера	1,3 МПикс, /встроенная лампа подсветки/ сменные видео объективы
Стандартный видеобъектив	F# 1,2/ *f* = 8 мм / FOV 32°

Представление изображения

Дисплей	Цветной ЖК дисплей с размером по диагонали 5,6 дюйма, (1024×800 пикселей)
Видоискатель	Встроенный, с изменяемым наклоном, цветной, с высоким разрешением (800×480 пикселей)
Выходной видеосигнал	RS170 EIA/NTSC или CCIR/PAL композитный видеосигнал, IEEE-1394 FireWire DV-цифровой видеосигнал

Измерение

Интервал температур	От –40°C до +500°C в двух диапазонах, до +2000°C – опция
Точность	±2°C или ± 2% от абсолютной температуры (в °C)
Повторяемость	±1°C или ± 1% от абсолютной температуры (в °C)
Режим измерения	Точка/вручную (до 10 перемещаемых точек), автоматическое снятие показаний максимальной или минимальной температуры в пределах участка измерения. Область (круг или квадрат, до 5 перемещаемых областей), изотерма (2), профиль, дельта (разность) Т.
Управление с помощью меню	Палитры (цвета побежалости, радуга, радуга HC (высокий контраст), черно-белая, черно-белая инвертированная), автоподстройка (непрерывная, ручная), загрузка палитр с карт SD или через USB, авто настройка (ручная/ постоянная/ на основе выравнивания по гистограмме), видео изображение на экране в режиме реального времени (Picture in Picture), галерея изображений
Сигнализация	Автоматическая сигнализация по любой выбранной функции измерения, звуковая/цветовая сигнализация выше/ниже заданного уровня, сигнализация по статической температуре или по температуре образца
Вводимые установки	Число/время, единицы измерения температуры °C/°F, язык, масштаб
Корректировка коэффициента излучения	Изменения коэффициента излучения от 0,01 до 1,0, поправка на отраженную температуру окружающего воздуха. Встроенная таблица коэффициентов излучения различных материалов
Коррекция пропускания атмосферы	Автоматическая, на основании введенных расстояния, температуры атмосферы, относительной влажности воздуха
Коррекция отраженной температуры	Автоматическая, на основании введенного значения
Коррекция температуры оптики	Автоматическая, по информации встроенных датчиков
Коррекция пропускания внешней оптики/ окна	Автоматическая, на основании задаваемых значений температуры и коэффициента пропускания оптики

Сохранение изображения

Тип	Съемные карты памяти формата SD-card (256 Мб в комплекте), встроенная память RAM для записи в формате AVI и последовательностей радиометрических изображений
Формат файлов – ИК	Радиометрический формат JPEG, 14 бит/ нерадиометрическая запись
Формат файлов – видимый диапазон	Стандартный JPEG, автоматически связывается с соответствующим ИК-изображением / возможно использование видео маркеров
Голосовые комментарии	30 сек. комментарий записывается совместно с ИК-изображением через проводную гарнитуру (,беспроводная гарнитура Bluetooth – опция)
Текстовые комментарии	Выбираются из списка стандартных, и сохраняется совместно с ИК-изображением

Сравнительные характеристики ОНВ-псевдобинокуляров

Основные характеристики	МОДЕЛИ			
	1ПН74	Кремль-1/2	Сова-Б1	GEO-NV-III-NG
Увеличение, крат * очки / бинокль с насадкой (объективом)	1/2,6*	1/4	1/4	1
Угол поля зрения, град	40	40/12	37/9,5	40
Угловое разрешение по оси, штр/мм	33–38	40–50	33/30	40
Фокусное расстояние, мм	25	25/100	25/100	25
Относительное отверстие объектива	F/1,4	–	–	F/1,1
Диаметр выходного зрачка, мм	8	–	7,5	5
Удаление (вынос) выходного зрачка, мм	15	–	14	20
Диапазон настройки по базе глаз, мм		Отсутст.	60–70	54–70
Диапазон диоптрийной наводки, дптр	64	64	65	64
Предел фокусировки	25-беск.	25-беск. /500-беск.	25-беск. / 150-беск.	30-беск.
Габаритные размеры: • ширина • высота • толщина (вдоль оптической оси)	 217/265 185 105	 – – –	 152/152 73/93 150/24	 180 165 120
Масса в снаряженном состоянии, г	800/ 1000	500+/600 маска – 250	700+/1300 маска –500	850

Сравнительные характеристики ОНВ-псевдобинокуляров (продолжение)

Тип источников питания	2 АА	2 АА	1 ТХЛ-316 (3В)	2 АА Alkaline
Время непрерывной работы, час	24	20	30	24
Рабочий диапазон температур	6 50	–	–	–
Заявленная изготовителем дальность наблюдения ростовой фигуры человека в условиях ЕНО//в полной темноте с ИК-подсветкой	200/300	200/400	150/300	–

Технические характеристики индикатора поля-частотомера SEL SP-71M «Оберег»

Диапазон частот	100–2800 МГц
Дальность обнаружения сотовых телефонов	до 20 м
Дальность обнаружения р/м P = 5 мВт	до 3 м
Динамический диапазон индикатора Уровня	не менее 44 дБ
Виды индикации	виброзвонок, световая, звуковая отключаемая
Питание	1,5 В (батарея ААА)
Время работы в сторожевом режиме	24 часа
Время работы в поисковом режиме	24 часа
Габариты	60×40×18 мм

Основные технические характеристики дифференциального детектора поля «АРК-ДДП»

Частотный диапазон	10 МГц..... 3 ГГц
Динамический диапазон	50 дБ
Подавление синфазного сигнала	55 дБ
Максимальная мощность входного сигнала	+20 дБм
Напряжение питания	9В от встроенного Ni-Ca аккумулятора 150 мАхч
Потребляемый ток	20 мА
Время заряда аккумулятора	15 часов
Габариты	10 МГц..... 3 ГГц

Зарядное устройство

Входное напряжение	220В/50 Гц
Выходное напряжение	12 В
Выходной ток	250 мА

Технические характеристки сканирующего приемника «AR 8200 V3»

Диапазон частот	500kHz – 3000MHz (Сплошное перекрытие)
Виды модуляции	AM, WAM, NAM, WFM, NFM, SFM, USB, LSB, & CW
Настройка	любой шаг кратный 50Hz
Чувствитель-ность	500kHz – 2.0MHz AM: 3.5uV (10db S/N) 2.0MHz – 30MHz SSB: 1.5uV (10dB S/N), AM: 2.5uV (10dB S/N) 30MHz – 470MHz SSB: 0.3uV (10dB S/N), AM: 0.7uV (10dB S/N) FM: 0.35uV (12dB SINAD), WFM: 1.00uV (12dB SINAD) 470MHz – 1GHz NFM: 0.5ouV (12dB SINAD), WFM: 1.50uV (12dB SINAD) 1.0GHz – 1.3GHz NFM: 1.00uV (12dB SINAD) 1.3GHz – 2.039GHz NFM: 2.50uV (12dB SINAD)
Каналы пямяти	1000
Банки памяти	40 банков
Скорость скани-рования	35+ каналов в секунду (максимум)
Поисковая ско-рость	35+ значений в секунду
PASS frequencies	50 на банк поиска, 50 VFO Search
Антенна	BNC
Энергетические требования	12 В / 1 А
Потребляемая мощность	190mA (номинальный режим), 145mA (режим ожидания), 25mA (экономичный режим)
Размер	61×143×39 мм
Вес	196 гр (335 гр с 4 батареями NiCad)

Анализатор спектра «FS 300»

– Диапазон частот 9 кГц – 3 ГГц
– Уровень фазовых шумов – 90 dBc (1 Гц)
– Интермодуляционные искажения: динамический диапазон > 70 дБ
– Отображаемый уровень шумов -120 дБм (300 Гц)
– Разрешение полосы пропускания от 200 Гц до 1 МГц
– Встроенный частотомер с разрешением 1 Гц
– Максимальный уровень входного сигнала + 33 дБм
– Цветной TFT дисплей
– Автоматические измерения через USB
– Хорошая система маркеров
– Внутренняя память позволяет записывать до 10 установок прибора и до 5 изображений спектра сигналов

Технические характеристики комплекса «RS Mobile L»

Диапазон контролируемых частот, МГц	– 0,01–3000
Динамический диапазон приемника в ВЧ тракте, Дб	– 65
Чувствительность приемника в режиме панорамного анализа, мкВ	– 1–2
Шаг перестройки приемника, МГц	– 8
Ширина полосы анализа, МГц	– 8
Скорость панорамного анализа, МГц/с	– 200 (12,5)
Дискретность анализа, кГц	– 200 (12,5)
Время сканирования частотного диапазона, мин	– 2,5–5
Скорость обмена (ПК-контроллер), кБит/с	– 115
Скорость обмена (контроллер-приемник), Бит/с	– 9600
Питание, В:	
– DC	– 9–18
– AC	– 176–264
Габаритные размеры в сложенном состоянии, см	– 46,5×35,9×17,8
Вес комплекса, кг не более	– 12
Условия эксплуатации комплекса:	
– температура окружающей среды	– +5+45
Потребляемая мощность, Вт	– не более 30
2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ КОНВЕРТЕРА RS/Lplus	
Полоса пропускания (–3дБ), КГц	– 0,6-16000
Чувствительность по линейному входу:	
полоса 12 КГц, С/Ш –3 дБ, мВ	– 2,5
Частота преобразования, МГц	– 110-150
Выходное сопротивление, Ом	– 50
Уровень гетеродина на выходе РЧ, дБм	– 60
Динамический диапазон по интермодуляционным искажениям, дБ	– 40
Коэффициент преобразования по сетевому входу, мкВ/В	– 160
Коэффициент преобразования по линейному входу, мкВ/В	– 1000

Состав и комплектация системы «СИГУРД»

В базовый состав системы «СИГУРД» входят:

- Анализатор спектра (по выбору пользователя).
- Интерфейс связи GPIB-USB2.
- Комплект измерительных антенн:
- АИ5-0 дипольная активная (0,009...2000 МГц).
- АИР3-2 рамочная активная (0,009...30 МГц).
- Специализированное программное обеспечение «СИГУРД-Интерфейс», «СИГУРД-Дельта» и «СИГУРД-Тест».
- Дополнительное оборудование:
- Портативный IBM-совместимый компьютер.
- Токовые трансформаторы для измерения в линиях:
- ТИ2-1 токосъемник (0,2...1000 кГц).
- ТИ2-2 токосъемник (0,009...30 МГц).
- ТИ2-3 токосъемник (0,009…300 МГц).
- Измерительные антенны:
- АИ5-1 дипольная активная (0,009...1000) МГц.
- АИ4-1 дипольная активная (0,1...2000 кГц).
- АИР3-1 рамочная активная (0,2...400 кГц).
- Широкополосный усилитель ШУ-3 (0,009...1250 МГц).
- Комплект управления тестами на исследуемой ПЭВМ по IrDA-каналу.
- Активный пробник для контактных исследований.
- Комплект адаптеров для контактных исследований интерфейсов ПЭВМ.

Технические особенности комплекса «Гриф АЭ 1001»

Состав

Базовый блок с персональным компьютером типа Notebook	1
Измерительный микрофон PCB с пред-усилителем	1
Вибродатчик	1
Антенна электрическая	1
Антенна магнитная	1
Защищенная акустическая система	1
Штатив с головкой под микрофон	1
Специальное программное обеспечение – 1 CD диск	1
Комплект документации	1
Укладочные чемоданы	1

Технические характеристики

Диапазон рабочих частот	300–10000 Гц, в перспективе – 5–24000 Гц
Количество каналов приема	3, в перспективе – 4
Входное сопротивление:	канал 1–600 Ом; канал 2, 3, 4 – 1 МОм
Подавление синфазной помехи при работе на линию	>70 дБ
Максимальное входное напряжение постоянного тока	100 В
Максимальное напряжение переменного тока	10 В
Подавление помех 50 Гц	до 140 дБ
Динамический диапазон в полосе пропускания 1 Гц	канал 1 – 160 дБ/175 дБ с усреднением; канал 2 – 140 дБ/155 дБ с усреднением; канал 3 – 110 дБ; канал 4 – 135 дБ
Эффективное значение собственных шумов в полосе пропускания 1 Гц,	канал 1 – 2 нВ; канал 2 – 9,5 нВ
Полосы пропускания прибора	1, 2, 4, 8, 16 Гц
Полоса обзора	300 Гц – 3,4 кГц; 300 Гц – 10 кГц
Напряжение питания микрофона	8–10 В
Тестовый сигнал с размахом 100 мВ	розовый шум в октавных и третьоктавных полосах – 0–3400 Гц; синусоидальный сигнал с плавной программной перестройкой 0–10000 Гц
Время непрерывной работы от аккумуляторов	6 час

Технические характеристики переносного комплекса измерения ПЭМИ «Навигатор-П6»

Тип исследуемых излучений	Электрические и магнитные (определяются типом используемых антенн)
Диапазон частот по электрической составляющей электромагнитного поля	от 0,1 до 26 000 000 кГц
Диапазон частот по магнитной составляющей электромагнитного поля	от 0,03 до 30 000 кГц
Диапазон частот при измерении наводок	от 0,03 до 100 000 кГц
Устанавливаемые полосы пропускания	0,01; 0,03; 0,1; 0,3; 1, 3, 10, 30, 100, 300 кГц
Предел основной абсолютной погрешности измерения частоты ПЭМИН (кГц)	Не хуже +/– одна установленная полоса пропускания.
Динамический диапазон измерения уровней ПЭМИН	не менее 82 дБ
Уровень собственных шумов (дБ относит. мкВ), не хуже	0, при полосе пропускания 1кГц на частоте 100мГц
Предел основной относительной погрешности измерения уровня ПЭМИН	
в диапазоне частот 0,1 кГц и выше	+/– 2
в диапазоне частот 0,03:0,1кГц	+/– 3
Типы детекторов	пиковый
Масса нетто (при использовании в качестве управляющей подсистемы ПЭВМ типа Notebook)	от 15,5 до 30 кг
Электрическое питание	220 В, 50 Гц
Потребляемая мощность	от 110 до 350 Вт
Рабочие условия эксплуатации:	
– температура окружающего воздуха	от 10 до 35 град. С
– относительная влажность воздуха (при температуре 25 град. С)	до 80%

Технические характеристики основного блока системы «ПКУ-6М»

Диапазон частот принимаемых сигналов, кГц	30…24500
Чувствительность в режиме приема сигналов АМ, мкВ	не хуже 10
Чувствительность в режиме приема сигналов ЧМ, мкВ	не хуже 3
Чувствительность в режиме обнаружения сигналов звуковой частоты, мкВ	не хуже 100
Точность измерения частоты, кГц	±2
Разрешающая способность спектроанализатора, кГц	0,3
Питание, В	6
Ток потребления, мА	не более 150
Вес прибора, кг	0,65

Технические характеристики ST 031 «ПИРАНЬЯ»

Высокочастотный детектор-частомер	
Диапазон рабочих частот, МГц	30–2500
Чувствительность, мВ	<2 (200 МГц – 1000 МГц)
	4 (1000 МГц – 1600 МГц)
	8 (1600 МГц – 2000 МГц)
Динамический диапазон, дБ	60
Чувствительность частотомера, мВ	<15 (100 МГц – 1200 МГц)
Точность измерения частоты, МГц	± 0,1
Сканирующий анализатор проводных линий	
Диапазон сканирования, МГц	0,01–15
Чувствительность, при с/ш 10 дБ, мВ	<0,5
Шаг сканирования, кГц	5(1)
Скорость сканирования, кГц	50–1500
Полоса пропускания, кГц	10
Избирательность по соседнему каналу, дБ	30
Режим детектирования	АМ, ЧМ
Допустимое напряжение в сети, В	600
Детектор ИК-излучения	
Спектральный диапазон, нм	770–1000
Пороговая чувствительность, Вт/Гц^2	10 (–13);
Угол поля зрения, град.	30
Полоса частот, МГц	5
Детектор НЧ магнитного поля	
Диапазон частот, кГц	0,3–10
Пороговая чувствительность, А/(м×Гц^2)	10(–5)
Виброакустический приемник	
Чувствительность, В×сек^2/м	1
Собственный шум в полосе 300–3000 Гц, мкВ	50

Технические характеристики ST 031 «ПИРАНЬЯ» (продолжение)

Акустический приемник	
Чувствительность, мВ/Па	> = 5
Диапазон частот, Гц	300–6000
Осциллограф и спектроанализатор	
Полоса пропускания, кГц	22
Чувствительность по входу, мВ	10
Погрешность измерений, %	1
Скорость вывода осциллограммы, с	0,2
Скорость вывода спектрограммы, с	0,3
Индикация	
Жидкокристаллический графический дисплей с разрешением 128×64 точки с регулируемой подсветкой	
Напряжение питания, В	6(4 батареи или аккумулятора типа АА)/220
Максимально потребляемый ток, не более, мА	300
Потребляемый ток в рабочем режиме, не более, мА	150

Технические характеристики комплекса «Спрут-7»

Технические характеристики	Значение технических характеристик
1. Частотный диапазон, Гц	1–20000
2. Диапазон частот фильтров, Гц: 1/1-октавные фильтры по ГОСТ 17168 1/3-октавные фильтры по ГОСТ 17168	 2–16000 2–20000
3. Диапазон измеряемых уровней звукового давления, дБ	24–130
4. Диапазон измерения общего виброускорения, $м \cdot с^{-2}$	0,01–708
5. Предел основной погрешности измерений: уровня звукового давления, дБ уровня виброускорения, дБ	 ±0,7 ±0,7
6. Пороговая чувствительность входного напряжения, нВ	100
7. Коэффициент усиления адаптеров-усилителей, дБ	20, 40 и 40, 60
8. Время работы от аккумуляторов, не менее, час.	7
9. Масса, кг	25

Технические характеристики нелинейного локатора «NR 900 EM»

Передатчик	
Частота	860 МГц
Выходная мощность	не менее 200 Вт (средняя мощность 0,13 Вт)
Диапазон регулировки мощности	10 дБ
Вид модуляции зондирующего сигнала	Амплитудно-импульсная
Приемники	
Частота	1720 МГц 2580 МГц
Чувствительность (с учетом цифровой обработки)	не хуже –123 дБ/Вт(–93 dBm) [при соотношении с/ш 6 дБ]
Антенна	
Тип поляризации	круговая
Коэффициент эллиптичности	не хуже 0,75
Коэффициент усиления приемной антенны передающей антенны нелинейного локатора	не менее 6 дБ не менее 8 дБ
Ширина главного лепестка диаграммы направленности	не более 40°
Уровень задних лепестков диаграммы направленности	не более –20 дБ
Индикация	
Звуковая:	тональный сигнал (250 Гц)
Визуальная:	4-х строчный ЖК индикатор
Отображаемая информация	уровень 2 гармоники (сегментная шкала и цифровое значение) уровень 3 гармоники (сегментная шкала и цифровое значение) разность уровней 2 и 3 гармоники (цифровое значение) значение аттенюаторов приемников индикация значения выходной мощности индикация подключения телефонов к приемнику на 2 или 3 гармонике символ режима подавления GSM напряжение аккумулятора

Технические характеристики нелинейного локатора «NR 900 EM»
(продолжение)

Имитатор	
Штатный имитатор	полупроводниковый диод 2Д521А
Дальность обнаружения имитатора на открытом пространстве (в режиме излучения максимальной мощности и максимальной чувствительности)	не менее 0,7 м
Точность локализации имитатора (в режиме минимальной мощности и минимальной чувствительности)	не хуже 0,1 м
Питание	
Сеть	220 В (50–60 Гц) (через адаптер)
Аккумулятор	12 В (два комплекта)
Время непрерывной работы от одного комплекта аккумуляторов	4 ч
Потребляемая мощность	не более10 ВА
Размеры	
Антенна	диам. 194 мм
Телескопическая штанга (максимальная длина)	980 мм
Блок приемопередатчика	215×162×63 мм
Прибор в транспортной упаковке	540×420×150 мм
Вес нелинейного локатора	
Телескопическая штанга с антенной системой	0,8 кг
Блок приемопередатчика	2,2 кг
Снаряженный прибор (с аккумулятором)	3,3 кг
Прибор в транспортной упаковке	8,4 кг
Условия эксплуатации нелинейного локатора NR 900 EM	
Диапазон рабочих температур	+5...+50 °С
Значения предельных пониженной и повышенной температур	–40°С ...+70 °С
Относительная влажность воздуха (при температуре +25°С)	не более 80%

Металлодетектор «АКА -7202М»

Технические характеристики	
МАХ дальность обнаружения металлических предметов, мм	
Монета диаметром 25 мм (сплав на основе меди)	450
консервная банка	1000
крупные объекты	2500
Режимы управления	
Динамический	да
Статический	да
автоматический программируемый	нет
ручной	нет
Режимы поиска	
все металлы	да
секторная дискриминация	да
Электрические характеристики	
напряжение питания, Вольт	12
Источник питания	Аккумулятор 1200 ма-ч
Время непрерывной работы, час	12
Условия эксплуатации	
Относительная влажность, %	98
при температуре, °С	25
атмосферное давление от	630 до 800 мм.рт.ст
Диапазон рабочих температур	–20°С до +50 °С или от 0 °С до +50°С (в зав. от индикатора)
Габаритные размеры	
Электронный блок, мм	138×108×75
Телескопическая штанга, мм	1200 (мах)
Датчик, мм	Ø260 или Ø215 мм
Потребительские характеристики	
Гарантия	2 года

Технические характеристики обнаружителя оружия «Рубеж-Д»

Вероятность обнаружения пистолета типа ПСМ – не менее 0,98;

Вероятность ложных срабатываний от набора предметов личного пользования общей массой до 200 г – не более 0,05

Пропускная способность – до 60 предметов в минуту;

Габариты контролируемой ручной клади:

- длина – 500 мм,
- ширина – 150 мм,
- высота – 360 мм;

Условия применения:

температура окружающей среды от +5 до+ 400 °С при относительной влажности до 85%

Размеры:

- высота панелей – 700 мм;
- общая ширина – 250 мм;

Масса – не более 16 кг;

Электропитание: – 60 ВА при переменном напряжении 220 В – 10%, 50 Гц.

Некоторые характеристики рентгенотелевизионной установки «НОРКА»

Излучатель	«РИ-100М»	«РИ-150М»
Максимальное напряжение на трубке, кВ	100	150
Размер фокусного пятна с дополнительной фокусировкой, мкм	40	80
Изделие позволяет обследовать внутреннее содержание контролируемых предметов толщиной (в эквиваленте по стали/алюминию),не менее, мм	12/50	20/80
Разрешающая способность изделия соответствует выявлению (без преграды) медной проволоки диаметром, мм	0,08	
ПРЕОБРАЗОВАТЕЛЬ РЕНТГЕНО-ТЕЛЕВИЗИОННЫЙ		
Блок телекамеры		
Аналоговый	«СКБ-2»	
Цифровой (разрешение, ppi / динамич. диапазон, бит)	«СКБ-2Д» (800x600/10)	
Блоки управления	Диагональ экрана	Объем памяти (количество изображений)
«БУ-2М»	6,4"	32; 64; 128
«БУ-4»	12"	10000
Питание		
от сети переменного тока, В/Гц	220/50	
автономное от аккумуляторной батареи	достаточно для 50 снимков	

Некоторые характеристики рентгенотелевизионной установки «НОРКА» (продолжение)

Излучатель	«РИ-100М»	«РИ-150М»
Максимальное напряжение на трубке, кВ	100	150
Размер фокусного пятна с дополнительной фокусировкой, мкм	40	80
Изделие позволяет обследовать внутреннее содержание контролируемых предметов толщиной (в эквиваленте по стали/алюминию),не менее, мм	12/50	20/80
Разрешающая способность изделия соответствует выявлению (без преграды) медной проволоки диаметром, мм	0,08	
ПРЕОБРАЗОВАТЕЛЬ РЕНТГЕНО-ТЕЛЕВИЗИОННЫЙ		
Блок телекамеры		
Аналоговый	«СКБ-2»	
Цифровой (разрешение, ppi / динамич. диапазон, бит)	«СКБ-2Д» (800x600/10)	
Конвертер, поле обследования, мм		
«ПР-1»	152×114	
«ПР-4»	250×190	
«ПР-5»	400×300	
«ПР-6»	550×410	
Блоки управления	Диагональ экрана	Объем памяти (количество изображений)
«БУ-2М»	6,4"	32; 64; 128
«БУ-4»	12"	10000
Питание		
от сети переменного тока, В/Гц	220/50	
автономное от аккумуляторной батареи	достаточно для 50 снимков	

Технические характеристики генератора шума «ГШ-1000»

Диапазон частот:	0,1...1000 МГц.
Индикация:	световая.
Спектральная мощность шума на расстоянии 1 м:	
0,1...100 МГц:	не менее 60 дБ;
100...300 МГц:	не менее 70 дБ;
300...500 МГц:	не менее 45 дБ;
500...1000 МГц:	не менее 25 дБ.

Генератор шума «ГШ-К-1000М»

Предназначен для защиты от утечки информации за счет побочных электромагнитных излучений и наводок средств офисной техники на объектах 2 и 3 категорий. Отличительные особенности – использование рамочной антенны для создания пространственного зашумления, установка в свободный слот персонального компьютера, выпускаются для слотов PCI и ISA. Изделие имеет сертификат Гостехкомиссии России.	
Диапазон частот	0,1–1000 МГц
Уровень шумового сигнала относительно 1 мкВ на расстоянии 1 м от антенны в диапазоне 0,1–1 МГц	не менее 46 дБ
Уровень шумового сигнала относительно 1 мкВ на расстоянии 1 м от антенны в диапазоне 1-100 МГц	не менее 48 дБ
Уровень шумового сигнала относительно 1 мкВ на расстоянии 1 м от антенны в диапазоне 100-1000 МГц	не менее 38 дБ
Коэффициент качества шума	не менее 0,8
Питание	220 В
Габариты	165×125×25 мм

Основные характеристики прибора «PRAGMA»

- симметричное шифрование по ГОСТ 28147-89;
- алгоритм речепреобразования – CELP 4800 бод;
- защита факсимильных документов путем шифрования передаваемого изображения, в защищенный факсимильный документ добавляется «шапка», внешний вид которой может задавать сам пользователь;
- защита факсимильных документов происходит автоматически, не требуя вмешательства пользователя;
- защита межкомпьютерного обмена данными;
- система открытого распределения ключей Диффи-Хеллмана (1024 бит) создает уникальный ключ для каждого сеанса связи и исключает необходимость ввода сеансовых ключей пользователем;
- введена система проверки подлинности, исключающая возможность вмешательства «третьей» стороны (атаки вида «человек посередине»), даже при наличии подобного устройства. Решается это применением алгоритмов «защищенные переговоры о согласовании ключа»;
- предусмотрена возможность смены ключевых и др. параметров работы устройства самим пользователем;
- для удобства пользователей: при необходимости оперативной смены ключевых параметров предусмотрен инжектор ключей, позволяющий ме-

нять ключевые параметры устройства. При этом осуществляется проверка на целостность ключевых параметров, предотвращающая несанкционированное навязывание параметров ключевой системы;

• исключена возможность влияния производителя устройства на систему защиты, организуемой пользователем.

Новые возможности

• Автономное питание «PRAGMA» позволяет пользователю создавать сети закрытой связи там, где Вы считаете необходимым. Нет зависимости от источника питания.

• Важно, что «PRAGMA» обеспечивает связь высокого качества не только на «близких» междугородних каналах, но и на «дальних»– международных, спутниковых. Кроме того, продукт оптимизирован для местных линий связи с большим затуханием и плохим соотношением сигнал/шум.

• По сравнению с шифраторами предыдущего поколения, усилена ключевая система– 1024 бит. Предусмотрен инжектор ключей, позволяющий оперативно менять ключевые параметры без подключения к компьютеру.

Технические характеристики анализатора линий «КОМ-2М»

– Анализатор линий позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных параллельно к линии, с мощностью потребления – 10 мкВт и более, оборудованных сторожевыми устройствами;

– анализатор позволяет обнаруживать блоки питания специальных радиоэлектронных устройств, подключенных последовательно к электросиловой линии, с мощностью потребления – 100 мкВт и более;

– напряжение испытательного сигнала (220±20)В; на частоте 50 Гц;

– чувствительность на второй и третьей гармонике испытательного напряжения не хуже – 10 мкВ;

– анализатор позволяет фиксировать отклонения импеданса линии от типового значения, при подключении к линии последовательно соединенных конденсатора с емкостью 100 пФ и более и резистора с сопротивлением 1 МОм ;

– диапазон измерения токов утечки от 0,1 до 200 мА;

– диапазон измерения сопротивления изоляции от 100 кОм до 20 Мом;

– анализатор позволяет определять нахождение обследуемой телефонной пары в телефонных распределительных шкафах;

– длина обследуемых линий – до 100 метров;

– питание от сети переменного тока напряжением 220 В частотой 50 Гц;

– габариты анализатора 220*200*70 мм;

– габариты штатной упаковки 360*360*140 мм;

– вес изделия в штатной упаковке 5 кг.

Генератор шума «Гром-4»

Сертификат Гостехкомиссии РФ

Предназначен для защиты от утечки информации за счет побочных электромагнитных излучений средств оргтехники, а также для создания помех устройствам несанкционированного съема информации с телефонных и электрических сетей.

Технические характеристики:

Пространственное зашумление в диапазоне 20–1000 МГц, мощность 5 Вт.

Линейное зашумление электросети в диапазоне 100–1000 кГц, мощность 4 Вт.

Использование эффекта «размывания» спектра акустического сигнала в телефонных линиях.

Независимая работа всех трех режимов.

Питание 220 В 50 Гц; мощность 25 Вт.

Устройство защиты телефонных переговоров от прослушивания и записи «ПРОКРУСТ ПТЗ-003»

Технические характеристики:

Максимальное поднятие постоянного напряжения на линии в режиме «Уровень» до 35В.

Амплитуда «белого» шума в режиме «Шум» до 10 В.

Диапазон шумового сигнала в режиме «Шум» 50 Гц...10 кГц.

Максимальная амплитуда помехи в режиме «ВЧ помеха» до 35 В.

Напряжение на диктофонном выходе регулируемое, до 10 мВ.

Питание сеть 220 В, 50 Гц.

Потребляемая мощность не более 10 Вт.

Габариты 64×157×205 м.

ПРИЛОЖЕНИЕ 2

НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО ПРОТИВОДЕЙСТВИЮ ТЕХНИЧЕСКОЙ РАЗВЕДКЕ

1. Законы Российской Федерации:

«О государственной тайне» от 21 июля 1993 г. № 5151-1.

«Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ.

«О безопасности» от 5 марта 1992 г. № 2446-1.

«О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. № 4524-1.

«О связи» от 16 февраля 1995 г. № 15-ФЗ.

«Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ.

2. Указы Президента Российской Федерации:

«Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. № 212.

«Вопросы защиты государственной тайны» от 30.03.1994 г. № 614.

«Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. № 1203.

«О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. № 1108.

«Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. № 71 с изменениями, внесенными Указами Президента Российской Федерации от 21 апреля 1996 г. № 573, от 14 июня 1997 г. № 594.

«О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. № 644.

«Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188.

3. Постановления Правительства Российской Федерации:

Инструкция № 0126-87.

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров –

Правительства Российской Федерации от 15 сентября 1993 г. № 921-51.

«Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. № 1233.

«О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. № 333.

«О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. № 513.

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. № 870.

«0б утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. № 973.

«О сертификации средств защиты информации» от 26 июня 1995 г, № 608.

4. Решения Гостехкомиссии России:

«Основы концепции защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам» от 16 ноября 1993 г. № 6.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации» от 14 марта 1995 г. № 32.

«Типовое положение о Совете (технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам» от 14 марта 1995 г. № 32.

«Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (учреждении, организации)» от 14 марта 1995 г. № 32.

«О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте» от 3 октября 1995 г. № 42.

«Методические рекомендации по разработке развернутых перечней сведений, подлежащих засекречиванию» от 3 февраля 1995 г. № 29.

«Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)» от 23 мая 1997 г. № 55.

«Положение о государственном лицензировании деятельности в области защиты информации (Решение Гостехкомиссии России и ФАПСИ)» от 27 апреля 1994 г. № 10 с дополнениями и изменениями, внесенными Решением Гостехкомиссии России и ФАПСИ от 24 июня 1997 г. № 60.

Положение о головной научно-исследовательской организации по проблеме защиты информации (Решение Председателя Гостехкомиссии России) от 15 марта 1993 г.

Пособие по проектированию технических мероприятий защиты военно-промышленных объектов от ИТР (Пособие к ВСН-01-82). Утверждено НИИА и согласовано с Гостехкомиссией СССР в 1983 г., переутверждено Решением Гостехкомиссии России от 13 ноября 1990 г, № 89-3.

«О защите информации при вхождении России в международную информационную систему «Интернет» от 21 октября 1997 г. № 61.

5. Руководящие и нормативно-методические документы Гостехкомиссии России:

Руководящий документ (РД). Защита от несанкционированного доступа (НСД) к информации. Термины и определения. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по ЗИ. Решение Председателя Гостехкомиссии СССР от 30 марта 1992 г.

РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение Председателя Гостехкомиссии России от 30 марта 1992 г.

РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 25 июля 1997 г.

РД. Защита информации Специальные защитные знаки. Классификация и общие требования. Решение Председателя Гостехкомиссии России от 25 июля 1997г.

Модель ИТР-2010. Решение Гостехкомиссии России от 16 августа 1996 г. № 49.

Методики оценки возможностей ИТР (МВТР-87) (с изменениями) Решение Гостехкомиссии СССР от 16 сентября 1987 г. №70-3, извещения № 1-88, № 2-90, № 3-91, № 4-93.

Нормативно-методические документы (НМД) по противодействию (ПД) средствам иностранной радиотехнической разведки. Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

Нормативно-методические документы по противодействию иностранной радиоразведке. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

Нормативно-методические документы по противодействию средствам иностранной фоторазведки и оптикоэлектронной разведки. Решение Гостехкомиссии СССР от 12 июня 1990 г. № 86-2.

Нормативно-методические документы по противодействию средствам иностранной гидроакустической разведки. Решение Гостехкомиссии России от 16 ноября 1993 г. № 7.

Нормативно-методические документы по противодействию радиолокационным средствам иностранной воздушной и космической разведок. Решение Гостехкомиссии России от 16 ноября 1993г. № 7.

Нормативно-методические документы по противодействию радиационной разведке. Решение Гостехкомиссии России от 15 ноября 1994 г. № 25.

Нормативно-методические документы по противодействию тепловизионным средствам иностранной инфракрасной разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной химической разведки. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной разведки лазерных излучений. Решение Гостехкомиссии России от 14 марта 1995 г. № 32.

Нормативно-методические документы по противодействию средствам иностранной акустической (речевой) разведки. Решение Гостехкомиссии России.1991 г.

Нормы эффективности защиты АСУ и ЭВТ от утечки информации за счет ПЭМИН. Решение Председателя Гостехкомиссии СССР, 1977 г.

Нормы эффективности защиты технических средств передачи телевизионной информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13, от 30 ноября 1987г. № 11-3.

Нормы эффективности защиты технических средств передачи телеграфной и телекодовой информации от утечки за счет ПЭМИН. Решение Гостехкомиссии СССР от 26 сентября 1977 г. № 13.