ШПИОНСКИЕ И АНТИШПИОНСКИЕ ШТУЧКИ
Яковлев В. А.

Яковлев В. А.

ШПИОНСКИЕ И АНТИШПИОНСКИЕ ШТУЧКИ

От скрытого наблюдения и прослушки до использования компьютера, смартфона и мобильного телефона в шпионских целях. И как такому вниманию противодействовать.

НиТ
издательство

В. А. Яковлев

Шпионские и антишпионские штучки. — СПб.: Наука и Техника, 2015. — 320 с.

ISBN 978-5-94387-846-6

Книга рассказывает об организации скрытого видеонаблюдения, выбора видеокамер, регистраторов и другого оборудования. Освещаются правовые вопросы создания, приобретения и использования шпионских штучек в нашей стране. Рассматриваются и антишпионские штучки, например, индикаторы поля, обеспечивающие обнаружение жучков, постановщики помех, «глушилки», созданные для предупреждения утечки информации.

Но главными шпионскими штучками нашего века могут стать ПК, планшеты, смартфоны, мобильные телефоны. Описаны программные комплексы, осуществляющие слежение за абонентом или пользователем. Такие программы предусматривают запись и прослушку телефонных разговоров, прослушивание окружения, перехват SMS или сообщений электронной почты, контроль местоположения, выявление паролей и пр. Рассматриваются и антивирусы-антишпионы, позволяющие обнаружить и уничтожить в ваших устройствах шпионские программы.

Для радиолюбителей будут интересны разделы книги о схемных решениях шпионских и антишпионских штучек. Схемы сопровождаются описаниями, рекомендациями по сборке и настройке. Все эти конструкции доступны домашним мастерам.

Книга предназначена для широкого круга читателей.

9 785943 878466

ISBN 978-5-94387-846-6

Контактные телефоны издательства
(812) 412-70-25, 412-70-26

Официальный сайт: www.nit.com.ru

ООО «Наука и Техника».
Лицензия № 000350 от 23 декабря 1999 года.
198097, г. Санкт-Петербург, ул. Маршала Говорова, д. 29.
Подписано в печать 28.01.2015 г. Формат 70×100 1/16.
Бумага газетная. Печать офсетная. Объем 20 п. л.
Тираж 1000. Заказ № 15.

Отпечатано с готовых диапозитивов
в ГП ПО «Псков-Полиграф».
180004, г. Псков, ул. Ротная, 34.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вполне легальная электроника в силу глобальной миниатюризации сегодня уменьшились до таких размеров, что легко может выполнять функцию электронных «насекомых». Сантиметровые диктофоны и видеокамеры — чем не идеальные «жучки»... Наши сограждане обожают подслушивать и подглядывать. Реальный спрос на подглядывающие и прослушивающие устройства в стране сегодня просто колоссален. Причем, как утверждают продавцы этой техники, восемь из десяти запросов на технику касаются не защиты от прослушки, а именно организации прослушки.

У современного человека существует множество проблем, связанных с различными сторонами его жизни. Своевременное получение необходимой информации — это залог успеха и осведомленность об окружающей обстановке. Часто бывают ситуации, когда просто необходимо узнать что-либо, но никак не получается справиться собственными усилиями в силу разных обстоятельств. В этот момент нам требуется помощь технических средств, **шпионских штучек**. В приобретении таких средств могут помочь специальные магазины шпионских штучек или магазины специальных гаджетов.

Сегодня, благодаря развитию новых технологий, появлению новых материалов, на рынке представлено изобилие портативной и миниатюрной электроники. Купить шпионскую технику, как у Джеймса Бонда, может позволить себе каждый.

Шпионские штучки в большинстве стран мира открыто продаются и в магазинах, и в Интернет-магазинах.

Это интересно знать.

*Сразу добавлю, что Россия и Украина к этому большинству не относится. Изготовление, продажа и **даже приобретение** большинства шпионских штучек у нас законодательство запрещает.*

В Тайване предлагается, например, бинокль, в который вмонтирован фотоаппарат. Им реально незаметно сфотографировать любой объект на расстоянии до километра, да еще при плохой видимости. Можно купить шпионскую зажигалку, ее главное назначение не зажигать сигареты, а подслушивать разговоры.

«*Если вы хотите узнать, о чем ведут разговоры ваши конкуренты,* — раскрывает тайванский продавец магазина Шпионских штучек, — *купите небольшие настольные часы. Время они показывают, но одновременно и слушают все вокруг, что позволяет тайно записать интересующую беседу*».

Помимо туристов, посетивших Тайвань, купить шпионские штучки хотят владельцы заводов, типографий, океанских судов и предприниматели во всех областях человеческой активности. Именно они платят $2000 за шариковую ручку или зажигалку, которые позволят им знать и предвидеть все подпочвенные течения, подмывающие основы бизнеса. Неудивительно, что в подобных условиях в повседневную практику деловой жизни входят скремблер.

Теперь перенесемся из Тайваня в Великобританию. В Лондоне в магазине Шпионских штучек продаются внешне ничем не примечательные чемоданчики. Покупают их отнюдь не для того, чтобы использовать по прямому назначению, так как свободного места в них практически нет. И к тому же цена чемоданчика — £3500.

В чемоданчике есть, например, специальный детектор для обнаружения взрывчатки, есть устройство, которое сигнализирует владельцу чемоданчика, что его подслушивают через умело спрятанные микрофоны. Для защиты от грубого насилия предназначена мощная сирена, которая включается тогда, когда кто-то пытается силой вырвать из рук этот обычный на вид чемоданчик.

В случае похищения чемоданчика вместе с его владельцем включается сигнальное устройство, которое поможет полиции определить местонахождение жертвы злоумышленников. И в самом крайнем случае, когда отступать уже некуда, чемоданчик можно легко сложить, превратив его в пуленепробиваемый щит. В набор входит и вспышка мощностью 5 мегаватт, чтобы ослепить нападающего (http://www.sudba.info/).

Современные шпионские штучки очень разнообразны по своему функциональному назначению и могут многое, в том числе дать возможность как отгородиться от посягательств на свою личную жизнь, так и наоборот.

Если нужно знать, о чем говорят в ваше отсутствие, то прослушка или «жучки» — это решение. Прослушка мобильного телефона также не редкость в наше время.

Если же что-то беспокоит в собственном доме, то скрытые мини камеры помогут разрешить все сомнения. Миникамеры могут быть легко установлены и в квартире, и в доме. Использование миникамеры открывает уникальные возможности. Например, можно узнать, как обращается няня с ребенком, чем занимаются близкие люди или же сотрудники в офисе. Таким образом, наша жизнь станет куда более интересной.

Чем больше появляется на рынке таких Шпионских штучек, как портативные видеокамеры для скрытого наблюдения, всевозможные «жучки», миниатюрные диктофоны и прочие шпионские штучки, тем больше следует обывателю знать о подобной технике, особенностях ее установки, наладки и функционирования, дабы не допустить утечки важных данных. Средства скрытого наблюдения в наше время столь миниатюрны, что случайно обнаружить их практически невозможно. Чем лучше вы осведомлены о том, какие шпионские вещицы представлены на рынке, тем лучше защищена от кражи ваша личная информация.

Разобраться в бесконечном разнообразии шпионских штучек в наши дни непросто, главным образом, потому, что производители представляют все новые и новые гаджеты различного назначения. В ответ на более изощренные способы прослушивания наших разговоров, все более совершенствуется защита от прослушки, появляются ее новые средства и методы.

Шпионские штучки — кто они? Различные шпионские штучки последнее время приобретают все большую популярность, поскольку все острее встает вопрос о сохранении собственной безопасности. Поэтому появляется множество магазинов, занимающихся реализацией шпионских штучек. Шпионские штучки обеспечивают **прослушивание** и **подсматривание**.

Все **устройства прослушки** условно делятся на четыре группы: «аудио жучки», радиостетоскопы, телефонные жучки и диктофоны. Легальны только последние. Приведу примеры.

Аудиожучок «Филин-1» ($25). Питается от батарейки 9 Вт и может передавать сигнал в условиях застройки до 100 м. На одной батарейке «жук» держится 20 дней, а «слышит» в радиусе 5—7 м. Принимать информацию желательно на спецприемник ($70).

Это интересно знать.

Если ловить сигнал от «жучка» на обычный радиоприемник, то откроется доступ к речевой информации всем обладателям радиоприемников в округе. Если же воспользуетесь спецприемником, то вещание будет проходить немножко выше или ниже стандартного FM-диапазона, соответственно, слушатели радио чужих тайн не услышат.

Радиостетоскопы предназначены для прослушивания разговоров через стены и оконные рамы. Ведь доступ к помещению для размещения там прослушки (причем в труднодоступных местах) может отсутствовать. Схема прослушки такая. Стетоскоп закрепляется скотчем на водопроводной/отопительной трубе (лучше ловящей вибрации голоса), расположенной в соседнем с прослушиваемым помещении. Сигнал принимается на спецприемник где-нибудь возле подъезда.

Радиостетоскоп МС-02 ($150) прослушивает стены толщиной до 0,8 м, оконные рамы с двойными стеклами, передавая сигнал на расстоянии до 100 м в условиях городской застройки. Без подзарядки функционирует несколько суток.

Телефонные «жучки» подключаются параллельно телефонной линии и питаются от нее, соответственно, исчезает необходимость в автономном питании.

Телефонный «жучок» ТР-1 ($40) прослушивает и телефонную линию, и помещение, даже когда телефонные разговоры не ведутся. Устанавливается либо в телефонный аппарат, либо в телефонную розетку. Сигнал передается либо в FM-диапазоне, либо на заранее оговоренной частоте.

Мини-диктофоны EDIC-mini TINY B21 (длина — 4 см, толщина — 1 см), **TINY B22** (длина 3,5 см, толщина 0,6 см) обладают немалой чувствительностью, записывая все в радиусе 7 м. Самый дешевый из диктофонов ($250) рассчитан на 18 часов записи, самый дорогой ($900) — на 300 часов, правда, через каждые 40 часов работы нужно менять батарейки. Благодаря функции голосовой активации эти диктофоны записывают лишь тогда, когда в помещении говорят, экономя при этом энергию и память.

Питающаяся от света модель **EDIC-mini TINY solar** (38×38 мм). Вариант мини-диктофона с памятью на 18 часов стоит $280, а с памятью 300 часов — $890.

Диктофон, вмонтированный в ручку ($249). В режиме записи сможет проработать до восьми часов.

Это интересно знать.
Основной недостаток прослушки при помощи диктофонов — необходимость повторного посещения помещения как для смены батареек, так и для окончательного изъятия устройства. Такая прослушка невозможна в режиме онлайн. Зато диктофон сложно (но можно) обнаружить средствами поиска, «жучки» же находятся последними без труда.

На рынке **устройств для «подсматривания»** наиболее популярны изделия из Китая, США, Кореи, России, Тайваня. Пример, беспроводная камера **LYD 203CA mini lens** (2×2 см, $105). Ее легко можно спрятать в мягкую игрушку (это незаконно), датчик движения или просто труднодоступное место. Имеет мини объектив, который невооруженным глазом разглядеть практически невозможно.

Портативный видеорегистратор mAVR-1 ($500) — изделие размером 5×5 см записывает до 50 часов видео. Недостатки этого варианта аналогичны недостаткам прослушки с диктофонами — для снятия информации придется повторно посещать помещение, кроме того, в режиме онлайн просмотреть ничего не получится.

Специальный видеоприемник ($99) обеспечивает «подсматривание» в режиме онлайн (с возможностью одновременной записи). Радиус вещания не превышает 30 м, канал связи не защищен. Недостаток в том, что все идущее в эфир смогут просмотреть все обладатели подобных видеоприемников в зоне его действия.

IP-камеры используют, чтобы исключить просмотр информации посторонними. Стоят они несколько дороже, да и по размерам больше. Но при этом взломать канал вещания и подключиться параллельно практически нереально. Покупают портативные камеры в основном не для промышленного шпионажа, а для охраны дома, офиса.

«Видеоняни» — это комплект из нескольких беспроводных камер и видеорекордера (от $250). Именно этому устройству эксперты предрекают наибольший рост популярности.

Антишпионские штучки — кто они? Антишпионские штучки предназначены для предупреждения утечки информации. Это индикаторы поля, обеспечивающие обнаружение аудио- и видео- жучков, диктофонов, а также постановщики помех, «глушилки» работающих шпионских штучек.

Антибаги или «жукоискатели». Сегодня достигнута стилизация «антибагов» под кредитные карточки, брелоки, ручки, зажигалки. **AntiBug Business ($145)** выполнен в виде зажигалки. Но по мнению профессионалов особого преимущества такая стилизация не дает. Такие стильные приборы могут лишь определить наличие излучателя сигнала в помещении. На подобных аппаратах нет шкалы уровня излучения, соответственно, нельзя определить, где находится прослушивающее устройство. Можно лишь узнать, что радиоизлучение «идет», Для определения месторасположения источника нужны полупрофессиональные устройства.

Полупрофессиональные антибаги — **AntiBug Profi** ($260), **BugHunter Apollo** ($550), **Hunter 2601** ($175), **Hunter Pro, BugHunter SP77**. А лучший из них Hunter Pro имеет наименьшие в своей категории размеры, металлический корпус, вибросигнал, который позволяет не смотреть на устройство при поиске «жука». То есть можно просто положить «охотника» в карман и ходить по комнате. Аппарат начинает вибрировать сразу, как только засечет «жучок», и чем ближе он будет к «насекомому», тем сильнее будет вибрация.

Однако все подобные устройства находят излучающие жучков, то есть использующих радиочастоту для передачи информации. Против проводных жучков или диктофонов они бессильны.

Глушилки или генераторы помех. Если нет возможностей на осмотр помещения профессионалами (например, в случае проведения непредвиденных переговоров в незнакомом месте), можно защититься при помощи активных средств — так называемых **генераторов шумов**. Эти устройства шипят, предоставляя средствам прослушки возможность слышать то же самое. Например, **Skeller** не больше спичечного коробка.

Для защиты телефонных разговоров чаще всего приобретают **ГРОМ ($520)**.

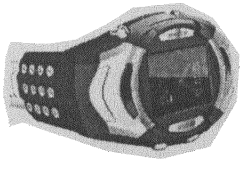
Большинство генераторов шумов «давят» до 70% голосовой информации. Полную защиту от прослушки может обеспечить генератор

сильного звукового шума **DRUID-248**, который полностью искажает речь. Участники разговора общаются через «коробку» системы — своеобразный «черный» ящик — при помощи микрофонов и наушников. Вместо слов и фраз человек без наушников (или «жучок») услышит только «булькающие» звуки. Единственный способ прослушать разговор — считать по губам.

Приведу несколько примеров «шпионских штучек».

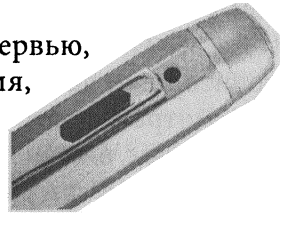
«Флешка-супердиктофон». Это, на первый взгляд, обычная **флешка емкостью 2 Гб** имеет очень чувствительный и мощный диктофон, который включается простым нажатием одной кнопки, не имеет никаких индикаторов и лампочек. Таким образом, это устройство практически невозможно отследить. Кроме этого всегда можно использовать этот диктофон как флешку по прямому назначению.

«Наручные часы-сотовый телефон». Дисплей: сенсорный 1,3″ дисплей, 160×128 пикселей, 260000 цветов. Время разговора: до 3 ч. Время в режиме ожидания: до 250 ч. Цвет: черный. Размеры: 62×46×18 мм. Вес: 90 гр. Батарея: Li-on 500 мАч. В комплекте имеется Bluetooth гарнитура стерео, проводная гарнитура стерео, USB кабель, зарядное устройство, аккумуляторы (2 шт.), Микро SD карта 1 Гб, инструкция (английский язык), стилус.



Ручка-камера (со встроенной 4 Gb памятью 720P HD) оснащена различными функциями: цифровой фотографией, видео- и аудио- записью, камера ПК, запись и хранение информации на флеш-накопителе. Ручка-камера включает в себя такие качества: изящный дизайн, удобство и портативность, простоту в использовании, устойчивость и надежность, быстроту реагирования.

Эта ручка хорошо подойдет для записи: интервью, аварии, спортивного рекорда, записи обучения, уголовного расследования и доказательства сбора для юридических целей, записи видео во время путешествия и т. д.



ГЛАВА 1

СКРЫТОЕ ВИДЕОНАБЛЮДЕНИЕ В КВАРТИРЕ И ЧАСТНОМ ДОМЕ

Видеонаблюдение давно применяется как способ защиты жизни и имущества, получения необходимой информации. Нынешние времена трудно назвать спокойными, поэтому организация безопасности квартиры и дома нуждается в особом подходе. Разумно камеры видеонаблюдения у себя дома устанавливать скрытно. Они не будут заметны для глаз посторонних людей и не будут портить интерьер помещения. Люди, устанавливающие скрытое видеонаблюдение у себя в жилище, стремятся огородить себя, своих близких, свою собственность от различных рисков.

1.1. Законность использования скрытого видеонаблюдения

Законодательные акты и Постановления

Скрытое видеонаблюдение — это съемка видеокамерами, которые не заметны посторонним. **Принцип работы** скрытой камеры видеонаблюдения очень прост — устройство располагается на определенном участке, далее через один из способов связи (радиоканал, провода или Интернет) соединяется с записывающим механизмом, а на монитор или накопитель направляется вся полученная информация. Просмотреть видео можно как в «прямом эфире», так и в записи.

Скрытое видеонаблюдение в ряде случаев может оказаться «вне закона». Опустим большинство нормативных актов, гарантирующих тайну личной жизни, рассмотрим **Постановление Правительства РФ № 214 от 10 марта 2000 г.**, определяющее запрещенные к применению технические средства систем видеонаблюдения.

Этот документ устанавливает также порядок ввоза в Российскую Федерацию и вывоза из нее юридическими лицами, не уполномоченными на осуществление оперативно-разыскной деятельности, специальных технических средств, предназначенных для негласного получения информации (далее именуются — **специальные технические средства**).

Это интересно знать.
На органы, осуществляющие оперативно-разыскную деятельность, определенные Федеральным законом «Об оперативно-розыскной деятельности», настоящее Положение не распространяется.

В документе отмечается, что порядок ввоза в Российскую Федерацию (вывоза из Российской Федерации) предусматривает:

- лицензирование ввоза в Российскую Федерацию (вывоза из Российской Федерации) специальных технических средств;
- таможенный контроль и таможенное оформление ввозимых в Российскую Федерацию (вывозимых из Российской Федерации) специальных технических средств.

Ввоз в Российскую Федерацию (вывоз из Российской Федерации) специальных технических средств осуществляется по лицензиям, выдаваемым Министерством промышленности и торговли Российской Федерации в установленном Правительством Российской Федерации порядке.

Для принятия решения о возможности ввоза в Российскую Федерацию (вывоза из Российской Федерации) специальных технических средств заявитель представляет в Центр соответствующее заявление, а также:

- техническую документацию на специальные технические средства;
- образцы специальных технических средств (по требованию Центра).

Ввозимые в Российскую Федерацию (вывозимые из Российской Федерации) специальные технические средства подлежат таможенному оформлению и таможенному контролю в соответствии с порядком, установленным законодательством Российской Федерации. Необходимым условием осуществления таможенного оформления и таможенного контроля специальных технических средств является наличие соответствующей лицензии Министерства промышленности и торговли Российской Федерации.

Список видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию, утвержденный постановлением Правительства РФ от 10 марта 2000 г. № 214 с изменениями и дополнениями от 27 ноября 2006 г., 8 декабря 2010 г., представлен в **табл. 1.1**.

Определение.
***ТН ВЭД ТС** (Товарная Номенклатура Внешнеэкономической Деятельности Таможенной Службы) — это общероссийский классификатор товаров, применение которого предусмотрено таможенным законодательством.*

В ТН ВЭД ТС представлена система классификации товаров, предназначенная для их кодирования и идентификации товаров при таможенной обработке. В настоящее время в таможенных органах используется ТН ВЭД ТС, которая построена на основе гармонизированной системы описания и кодирования товаров, используемой в мировой практике.

Для точного определения кода товаров необходимо использовать три составные части ТН ВЭД ТС:

- номенклатурную часть;
- примечание к разделам и группам;
- основные правила интерпретации.

Список видов специальных технических средств, ввоз и вывоз которых подлежат лицензированию *Таблица 1.1*

Наименование	Код ТН ВЭД ТС
Специальные технические средства для негласного получения и регистрации акустической информации: системы проводной связи, предназначенные для негласного получения и регистрации акустической информации; радиоаппаратура, предназначенная для негласного получения и регистрации акустической информации	из 8517 61 000; из 8517 62 000; из 8517 69 390 0; из 8517 69 900 0; из 8525 50 000 0; из 8527
Специальные технические средства для негласного визуального наблюдения и документирования: а) фотокамеры, обладающие, по крайней мере, одним из следующих признаков: закамуфлированные под бытовые предметы; имеющие вынесенный зрачок входа (pin-hole); без визира; с вынесенными органами управления камерой; б) телевизионные и видеокамеры, обладающие, по крайней мере, одним из следующих признаков: закамуфлированные под бытовые предметы; имеющие вынесенный зрачок входа (pin-hole); работающие при низкой освещенности объекта (0,01 лк и менее) или при освещенности на приемном элементе 0,0001 лк и менее; в) комплекс аппаратуры передачи видеоизображения по кабельным, радио и оптическим линиям связи	из 9006 51 000 0; из 9006 52 000 9; из 9006 53 100 0 из 8525 80 из 8517 61 000; из 8517 62 000; из 8517 69 390 0; из 8517 69 900 0; из 8525 50 000 0; из 8527

Таблица 1.1 (продолжение)

Специальные технические средства для негласного прослушивания телефонных переговоров: системы проводной связи, предназначенные для негласного прослушивания телефонных переговоров; радиоаппаратура, предназначенная для негласного прослушивания телефонных переговоров	из 8517 61 000; из 8517 62 000; из 8517 69 390 0; из 8517 69 900 0; из 8525 50 000 0; из 8527
Специальные технические средства для негласного перехвата и регистрации информации с технических каналов связи	из 8471; из 8517 61 000; из 8517 62 000; из 8517 69 390 0; из 8517 69 900 0; из 8523 40 200 0; из 8523 29 210 1; из 8523 29 210 2; из 8523 40 700 1; из 8523 51 700 1; из 8523 59 910 1; из 8523 80 910 1; из 8527
Специальные технические средства для негласного контроля почтовых сообщений и отправлений	из 9022 19 000 0
Специальные технические средства для негласного исследования предметов и документов переносная малогабаритная рентгеноскопическая и рентгенотелевизионная аппаратура	из 9022 19 000 0
Специальные технические средства для негласного проникновения и обследования помещений, транспортных средств и других объектов: средства для вскрытия запирающих устройств; переносная малогабаритная рентгеноскопическая и рентгенотелевизионная аппаратура	из 8301 70 000 0; из 9022 19 000 0
Специальные технические средства для негласного контроля над перемещением транспортных средств и других объектов	из 8526 10 000 9; из 8526 91
Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи	из 8471; из 8505 90 100 0; из 8517 61 000; из 8517 62 000; из 8517 69 390 0; из 8517 69 900 0; из 8523 40 200 0; из 8523 29 210 1; из 8523 29 210 2; из 8523 40 700 1; из 8523 51 700 1; из 8523 59 910 1; из 8523 80 910 1; из 8527
Специальные технические средства для негласной идентификации личности, многоканальные регистраторы психофизиологических реакций человека	из 9019 10 900 9

Это интересно знать.

Специальные технические средства могут быть как закамуфлированными под бытовые предметы, так и незакамуфлированными, если это не указано специально. Специальные технические средства, предназначенные для негласного получения информации, определяются наименованием и кодом товара по ТН ВЭД ТС.

Определение степени запрещенности технических средств

Установка скрытого видеонаблюдения является целесообразной в двух случаях:

- для обеспечения вандалостойкости системы;
- для создания условий, препятствующих определению зоны обзора видеокамеры.

Скрытая установка видеонаблюдения всегда являться положительным дезориентирующим фактором. К **запрещенным законодательно** средствам относятся камеры скрытого видеонаблюдения:

- закамуфлированные под бытовые предметы, имеющие вынесенный зрачок входа (pin-hole);
- работающие при уровнях освещенности ниже определенного уровня;
- устройства передачи изображения по различным каналам связи — кабельным, оптическим, радио.

Однако, указанный тип объектива камер видеонаблюдения pin-hole, не является достаточным основанием для их отнесения к устройствам негласного получения информации. Но при возникновении конфликтной ситуации последнее слово остается за экспертизой, а здесь все может быть неоднозначно.

Это интересно знать.
Реально отнесение скрытого видеонаблюдения к системам негласного получения информации целиком и полностью остается за правоохранительными и судебными органами. Понятие «скрытое видеонаблюдение» в этом законодательном акте не используется.

А какие системы скрытого видеонаблюдения можно использовать **относительно законно**?

Вывод.
Скрытые камеры видеонаблюдения, установленные в стены или потолки являются оптимальным вариантом, главным образом потому, что эти конструкции нельзя отнести к бытовым предметам.

Важен и **тип объектива.** Чтобы не доказывать свою правоту в суде, смотрим в упомянутом выше Постановлении **коды ТН ВЭД**, под которые подпадают запрещенные технические средства, и видим напро-

тив видеокамер такую запись «из 8525 80». Затем выбираем для скрытого видеонаблюдения камеру, код которой лежит вне указанного. Например, видеокамера KPC-S20PH4 имеет объектив *pin-hole* (англ. *игольное ушко*, **рис. 1.1**) и код ТН ВЭД 8531103000 (указан в сертификате соответствия). При таком подходе вопросов у правоохранительных органов быть не должно.

Рис. 1.1. *Внешний вид камеры с объективом pin-hole KPC-S190SP4-4,3*

Будьте осторожны.
Не забудьте также, что чувствительность выбираемой камеры скрытого видеонаблюдения должна быть более 0,01 лк для освещенности на объекте и более 0,0001 лк для приемного элемента видеокамеры.

Аналогичным образом следует поступить при выборе другого оборудования видеонаблюдения, при этом рекомендую пользоваться данными официальных изданий соответствующих документов.

С технической точки зрения монтаж скрытого видеонаблюдения более трудоемок, камеры видеонаблюдения, установленные скрыто, имеют ограниченные возможности регулировок в процессе эксплуатации, замена вышедшей из строя видеокамеры тоже представляет определенные сложности. Поэтому, принимая решения об установке скрытого видеонаблюдения, это стоит учесть.

Подведу итоги. Согласно законодательству продажа и монтаж скрытого видеонаблюдения уголовно наказуемо. А именно, запрещены «специальные технические приспособления для негласного визуального наблюдения», это «видеокамеры, обладающие, по крайней мере, одним из признаков:

- спрятанные в муляжах бытовых предметов;
- имеющие вынесенный зрачок объектива (pin-hole);
- снимающие при низкой освещенности объекта (0,01 лк и менее) или при низкой освещенности на приемном элементе 0,0001 лк и менее.

Под запрет этого закона **не подпадает видеоглазок (рис. 1.2)**, хоть он и имеет сходство с дверным глазком, он не является «муляжом бытового предмета». Также, закон не запрещает, если скрытая камера видеонаблюдения размещена в корпусе пожарного или охранного дат-

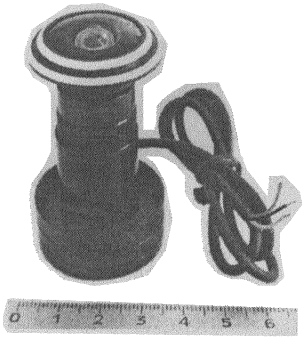


Рис. 1.2. Внешний вид видеоглазка

чика. Такие датчики относятся к системе безопасности и не являются бытовыми устройствами.

Как и любой закон, он имеет свои **недостатки**. Хоть и запрещена установка скрытых камер видеонаблюдения в бытовые приборы, но установку в стены, откосы, дверные проемы, потолок, двери **закон не запрещает**.

Где можно устанавливать скрытое видеонаблюдение, а где нет? Разрешена скрытая съемка своей собственности — в доме, квартире, на даче, в машине и т. д.

Хотя если вы решили установить скрытое видеонаблюдение в квартире, чтобы проследить за няней, женой или рабочими, то они вполне могут подать в суд на вторжение в личную жизнь. Но ни одного такого дела пока еще не открывали, да и доказать законность скрытого видеонаблюдения в своей квартире не составит труда даже начинающему адвокату.

Это интересно знать.
Также надо учитывать, что при скрытой съемке дачи, частного дома или коттеджа в объектив камеры не должны попадать соседние дома и участки.

Чтобы использовать скрытое видеонаблюдение в офисе необходимо предварительно взять письменное заявление со своих работников о том, что ведется видеонаблюдения и что они не имеют к этому претензий. А на входе в офис необходимо поместить табличку или стикер, которые будут информировать о видеонаблюдении.

Устанавливать скрытое видеонаблюдение в подъезде, на улице, на стоянке нельзя. Любое скрытое наблюдение в общественных местах на территории России можно только с разрешения суда. Выход из этой ситуации — устанавливать обычные (не скрытые) камеры наблюдения, разместить информационные таблички о том, что ведется наблюдение.

Любое видеонаблюдение в раздевалках, туалетах, душевых, саунах, банях и т. д. — строго запрещено!

Совет.

*Если не хотите организовывать скрытое видеонаблюдение, и в комнате есть компьютер — поставьте обычную вебкамеру и специальные программу для наблюдения (например, Webcam Surveyor, http://www.webcamsurveyor.com/ru/, **рис. 1.3**). Программа Webcam Surveyor подробно рассмотрена на сайте производителя.*

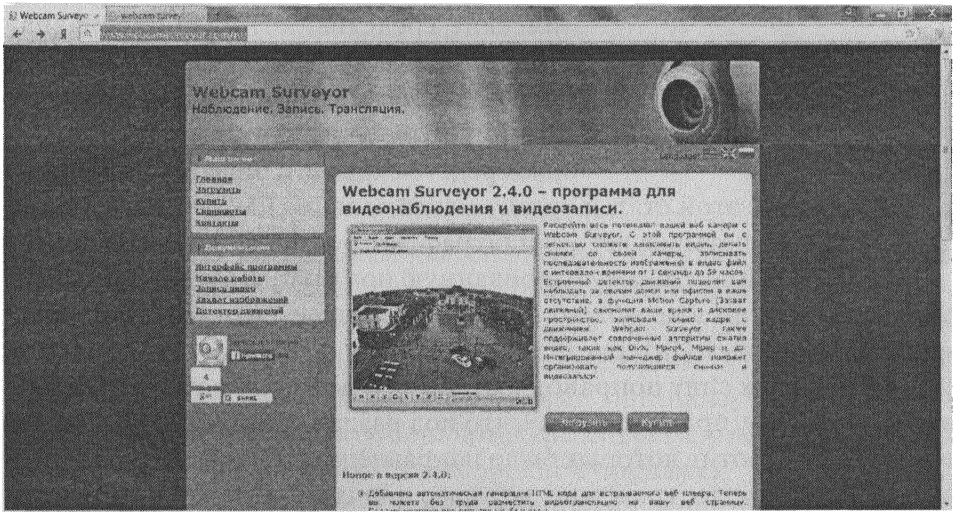


***Рис. 1.3.** Главная страница сайта программы Webcam Surveyor, русскоязычная версия*

Легальность Wi-Fi системы видеонаблюдения. По законодательству Российской Федерации использования таких систем разрешено только внутри помещений (офисов, складов, производственных территорий). Но если вы хотите установить Wi-Fi видеонаблюдение за пределами внутренних помещений, то придется обращаться в специальную службу, которая выдает лицензии на их использование.

Скрытое видеонаблюдение — это съемка видеокамерами, которые не заметны посторонним. А значит идеальный вариант для размещения камеры в привычных предметах (**рис. 1.4**) — в бытовой технике, в предметах интерьера, либо в муляже любого предмета, однако, как отмечалось выше, это запрещено законодательством.

Основополагающий документ — это Уголовный кодекс от 13.06.1996 г. РФ №63-ФЗ. Разберемся о чем он говорит:

Статья 137 говорит о том, что в России наказуем сбор и распространение сведений о частной жизни человека без его согласия, которые являются его личной тайной или тайной его семьи.

Рис. 1.4. Скрытая камера, встроенная в наручные часы

Статья 138 говорит о том, что в России наказуемо нарушение тайны телефонных переговоров, переписки, почтовых, телеграфных или иных сообщений.

Статья 138.1 говорит о том, что в России нельзя незаконно покупать, изготавливать и продавать специальные технические средства, которые предназначены для получения негласной информации (то есть без предупреждения тех людей, которых вы записываете с помощью средств скрытого видеонаблюдения), и за нарушение этой статьи грозит максимальное наказание лишение свободы аж до четырех лет (или штраф до трехсот рублей).

За скрытую или «закамуфлированную под бытовой предмет» видеокамеру в России уже можно попасть в тюрьму. Есть тому уже примеры, о чем пишет Интернет.

Вступление в силу **поправок к ст. 138 УК**, которые начали действовать в 2010 году, привело к тому, что под раздачу попали не шпионы и террористы, против которых было направлено законодательное нововведение, а простые граждане, которые понятия не имели о запретах, сообщает «Российская газета».

В этой статье УК говорится о запрете продавать и производить без специального разрешения так называемую «спецтехнику для скрытого наблюдения».

Часть 3 138-й статьи УК звучит так: «*Незаконные производство, сбыт или* ***приобретение*** *специальных технических средств (в том числе — видеокамеры, закамуфлированные под бытовые предметы), предназначенных для негласного получения информации, наказываются штрафом в размере до двухсот тысяч рублей либо лишением свободы на срок до трех лет*».

Новым в статье стало слово «***приобретение***». То есть теперь статья предписывает наказывать людей не только за нелегальное производство или продажу шпионских устройств, но и за их покупку. А так как российские суды обычно придерживаются обвинительного уклона, результат получился ошеломляющим.

Нас сегодня окружают сотни тысяч электронных глаз, фиксирующих каждый шаг. Установлены они и в открытом варианте, и скрытно. Сделано это для нашей же безопасности. Любой гражданин имеет

право обезопасить родное жилище и оснастить его системами наблюдения, в том числе и замаскированными под обычный дверной глазок. Однако на основании 138-й статьи теперь это можно трактовать как уголовно наказуемое деяние.

Проблема еще и в том, что найти подробный **список запрещенных устройств** невозможно. В Центре по лицензированию, сертификации и защите государственной тайны, который уполномочен осуществлять контроль над оборотом спецтехники, корреспонденту «Российской газеты» заявили: «*Представить исчерпывающий перечень признаков принадлежности изделий к специальной технике скрытого слежения не представляется возможным, так как подобный перечень не предусмотрен нормативными документами, регулирующими производство и оборот подобных приборов*».

Правда, существует постановление правительства РФ №214 от 10 марта 2000 года, но в нем классификация признаков спецтехники очень туманна. До сих пор, например, законодательством не определены признаки типа «камуфлированность», «бытовой предмет».

Например, постановление относит к категории спецтехники фотокамеры вроде Canon 5D с вынесенными органами управления. А подобная функция есть у большинства современных компактных фотоаппаратов, находящихся в свободной продаже.

Ноутбуки с встроенной видеокамерой и выходом в Сеть прямо подходят под определение «комплекс аппаратуры передачи видеоизображения по кабельным, радио- и оптическим линиям связи».

Теперь сделаем полезные и понятные **выводы**.

Вывод 1. Нужно знать законы и научиться дружить с ними. Если написано, что нельзя камуфлировать видеокамеры в бытовых предметах, значит не надо этого делать. Камуфлируйте их в дверях, стенах, дверных косяках, пожарных и охранных датчиках, которые являются частью здания, охранной и пожарной систем сигнализации, а система безопасности никогда не являлась бытовым предметом.

Вывод 2. Будьте осторожны при заказе через Интернет-магазины из Китая интересных технических штучек, обеспечивающих скрытое видеонаблюдение с помощью брелков, авторучек, часов и пр. Возможно, они запрещены для свободного использования, покупки и продажи на территории России.

Вывод 3. Устанавливайте китайские «pin-hole» видеокамеры, находящиеся в свободной продаже на территории России, в качестве дверных глазков. При этом обращайте внимание на светочувствительность.

Вывод 4. Действующий закон, касающийся скрытого видеонаблюдения, устарел, потому что многие технические новинки, заполнившие нашу жизнь, без которых мы уже и не мыслим комфортного существования, начинают подпадать под ограничения этого закона. То, что считалось раньше специальными средствами, сейчас используется уже как игрушка, например, встроенная видеокамера в защитный шлем велотрекера, в сотовый телефон, в планшет, в ноутбук, в солнечные очки или в подводную маску.

Вывод 5. За нарушение закона, в нашем случае, у нас уголовная ответственность. Получается, что на многие вещи сейчас закрываются глаза. Но если кому-то надо предусмотренное наказание применить, это может быть сделано. Поэтому будьте осторожны, ведь скрытое видеонаблюдение, в том числе инсталляция и использование, могут принести некоторые проблемы.

1.2. Организация скрытого наблюдения в квартире

Видеонаблюдение перед квартирой

В последнее время возросла роль видеонаблюдения за лестничной площадкой перед входной дверью в квартиру. Видеонаблюдение за лестничной площадкой наиболее полезно и оправданно с точки зрения возможных рисков. Ведь, как правило, видеонаблюдение нужно для того, чтобы обезопасить себя от нежелательного вторжения на территорию, а происходит это, за редкими исключениями, через входные двери.

Видеонаблюдение перед квартирой позволит избежать многих негативных ситуаций. После его установки родители могут быть уверены, что ребенок не откроет дверь квартиры незнакомцу, что все происходящие у входной двери события будут тщательно зафиксированы системой видеонаблюдения.

В наших условиях при звонке в дверь можно чувствовать себя относительно спокойно, если наблюдаешь из квартиры всю лестничную площадку от пола до потолка, а желательно и лестничные марши. При скудности освещения наших подъездов потребуется невидимая инфракрасная подсветка с дальностью не менее 3–4 м по всему углу

зрения видеоглазка. Источник освещения по известным причинам также должен быть максимально замаскирован. Такие требования жизни подтолкнули к широкому использованию инфракрасной подсветки с закамуфлированными источниками излучения.

Это интересно знать.

*В ряде случаев, если по конструкции лестничной клетки имеется большая мертвая зона видеоглазка и видеодомофона, используется дополнительное скрытое видеонаблюдение для полного контроля происходящего на лестничной площадке перед входной дверью (**рис. 1.5**).*

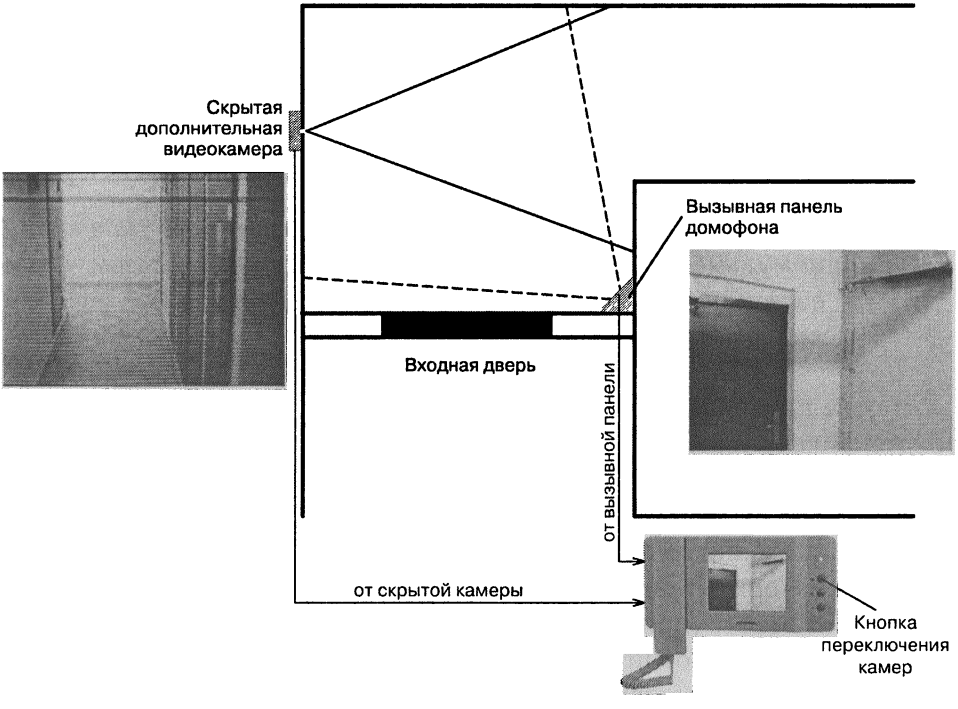


***Рис. 1.5.** Схема размещения элементов системы наблюдения с двухканальным видеодомофоном и дополнительной скрытой в стене камерой*

Самое распространенное решение — использование видеодомофона. **Видеодомофон** — это простое и удобное устройство, позволяющее контролировать доступ в помещение и вести наблюдение за пространством перед входной дверью или другими местами. Простейший

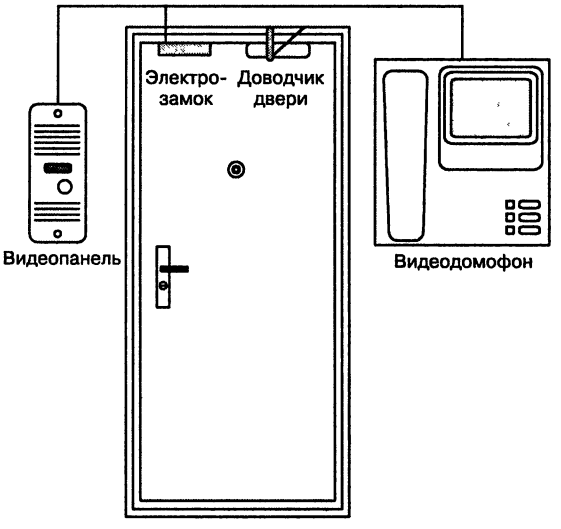


Рис. 1.6. Схема размещения элементов простейшей схемы с видеодомофоном

видеодомофон включает в себя вызывную панель и видеомонитор с небольшим экраном (**рис.1.6**).

Вызывная панель устанавливается снаружи рядом с входной дверью. Имеет камеру, микрофон и кнопку вызова, при помощи которой посетитель может известить о своем приходе. При нажатии кнопки сигнал вызова передается на монитор видеодомофона, раздается звуковой сигнал вызова.

Это интересно знать.

Иногда видеодомофоны снабжаются двумя-тремя миниатюрными камерами, тогда они настраиваются таким образом, чтобы видеть посетителя с разных ракурсов (например, анфас, три четверти и профиль).

Также видеодомофон может быть оснащен блоком памяти, тогда будут фиксироваться изображения всех людей, которые приходили к вам домой в ваше отсутствие.

Видеодомофоны при наличии дополнительных устройств, подключаемых к ним, позволяют:

- производить осмотр пространства перед входной дверью в полной темноте (при наличии ИК-прожетора);
- производить отпирание двери дистанционно (при монтаже специального электромеханического или электромагнитного замка на дверь, **рис. 1.7**);
- производить автоматическую запись в память устройства изображений посетителей, во время отсутствия хозяев нажавших на кнопку вызова (при монтаже устройства «image memory»).

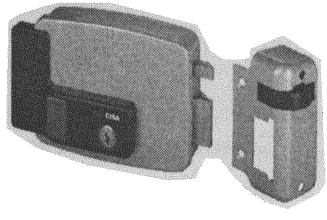


Рис. 1.7. Внешний вид электромеханического замка

При монтаже дополнительных коммуникационных устройств монитор видеодомофона можно совместить с телевизором, телефоном, компьютером, пейджером или радио.

Второй вариант — использование **видеоглазка** (подробнее рассмотрен в следующем разделе). Это миниатюрная видеокамера, которая крепится в том месте, где и обычный глазок. По внешнему виду с наружной стороны двери он ничем не отличается от обычного дверного глазка, но позволяет дистанционно следить за тем, что происходит на вашей площадке, а также вести запись на видеонакопители. Подобные системы имеют угол обзора объектива до 180 градусов. Иногда видеоглазок оснащают устройством инфракрасной подсветки для идентификации человека в темное время суток.

Но видеоглазок, как и простой глазок, можно залепить пластилином, тогда польза от него будет небольшая. Поэтому лучше использовать миниатюрные СКРЫТЫЕ камеры с объективом класса **pin-hole** (англ. — *игольное ушко*). Такая камера может быть вмонтирована в стену, заметить ее крайне трудно, если монтаж проводят грамотные специалисты.

Это интересно знать.

Pin-hole камеры также можно использовать и внутри квартиры в случае, если вы хотите вести видеонаблюдение, скажем, за домашним персоналом, при этом вам нужно сохранить втайне от персонала сам факт видеонаблюдения.

Более полный вариант — **комплексная система** (видеонаблюдение + сигнализация + домофон). Особенность в том, что совместно с системой видеонаблюдения используется система сигнализации и домофон (видеодомофон или аудиодомофон).

Комплексная система (рис. 1.8) решает такие задачи:

- полный видеоконтроль квартиры и пространства перед дверью;
- возможность видеозаписи длительностью до нескольких недель;
- хорошая видимость в условиях плохого освещения;
- быстрый поиск информации с высокой точностью — по времени, дате;
- отправка голосовых или текстовых сообщений на телефон при возникновении «тревожной ситуации».

Такая система позволяет контролировать квартиру, подъезд и пространство перед дверью, а в случае попытки проникновения активи-

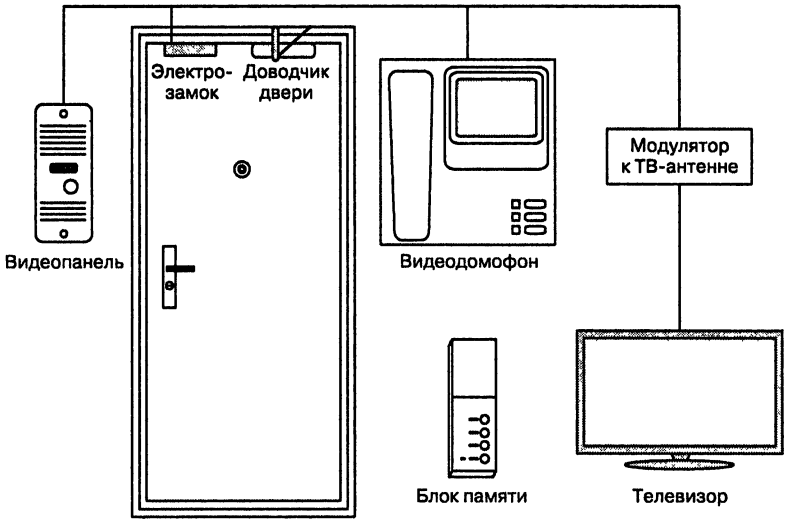


Рис. 1.8. Схема расширенного варианта видеонаблюдения перед входной дверью квартиры

ровать сирену, отправить «тревожное сообщение» на сотовый телефон, сообщить в пункт централизованного наблюдения.

На входную дверь устанавливается или видеодомофон, или видеоглазок. При необходимости устанавливаются датчики движения. Используется цифровое или аналоговое видеонаблюдение, цветные или черно-белые видеокамеры. Возможно цифровое улучшение изображения в условиях плохой видимости.

Это интересно знать.
Количество и расположение видеокамер подбирается в зависимости от конфигурации наблюдаемой квартиры.

В видеосистеме используются видеорегистраторы или видеомагнитофоны для записи информации. Если производится запись информации, то устанавливается специальное программное обеспечение, которое настраивается таким образом, чтобы облегчить и ускорить процесс поиска необходимой информации по времени и дате.

В случае тусклого освещения подъезда используется встроенная видеокамера (видеоглазок) **с ИК подсветкой**. ИК подсветка не видна глазу, но при этом хорошо освещает наблюдаемый объект. Внешний вид миниатюрного ИК-прожектора представлен на **рис. 1.9**.

Рис.1.9. Внешний вид миниатюрного ИК-прожектора

Для наблюдения пространства перед дверью устанавливается видеодомофон, видеоглазок и/или видеокамера.

С комплексной видеосистемой устанавливаются **датчики движения** для фиксации перемещения в области видимости камеры и для принятия необходимых мер.

Установка GSM видеонаблюдения позволяет при возникновении «тревожной ситуации» автоматически посылать текстовые или голосовые сообщения на телефон.

Видеоинформация с камер может поступать как на отдельный монитор, так и на обычный телевизор.

Есть возможность выводить на один монитор видеоинформацию от нескольких камер. Видеомониторы работают в автоматическом режиме, переключая изображение с разных камер, либо отображают видеоинформацию одновременно, при этом имеется возможность переключиться на необходимую камеру.

Дверные видеоглазки

Видеоглазок, как специализированная телекамера, имеющая наружный внешний вид типового дверного глазка и расположенная в двери вместо него, по сути, является чисто российским изобретением (**рис. 1.10**). Его появление в нашей стране обусловлено, как нам кажется, очевидными социально-экономическими и историческими факторами, сложившимися в России в последнее десятилетие прошлого века.

Прежде всего — эта камера для скрытой установки, а скрытая установка оборудования широко распространена в России отнюдь не от поголовной «шпиономании», а в результате стремления сохранить оборудование и оградить его от изощренного отечественного вандализма. На Западе население довольствуется видеодомофонами (отмечает *Н. Чура* в журнале «Специальная техника»).

Дверной видеоглазок является достаточно сложным радиоэлектронным прибором. Он состоит из миниатюрной камеры видеонаблюдения с ПЗС-матрицей и специального объектива, адаптированного для крепления в дверь (**рис. 1.11** и **рис. 1.12**).

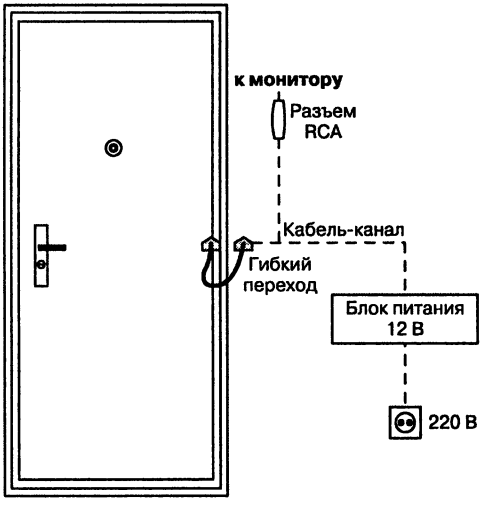


Рис. 1.10. Элементы видеонаблюдения перед входной дверью на базе видеоглазка

С наружной стороны двери видеоглазок внешне ничем не отличается от обычного дверного глазка, поэтому он не привлекает к себе особого внимания.

Первые видеоглазки, появившиеся у нас в первой половине 90-х годов, представляли собой бескорпусную моноплатную ПЗС-видеокамеру черно-белого изображения с типовым встроенным объективом. С наружной стороны двери объектив был скрыт за декоративным элементом от обычного дверного глазка. Кроме абсолютно недостаточ-

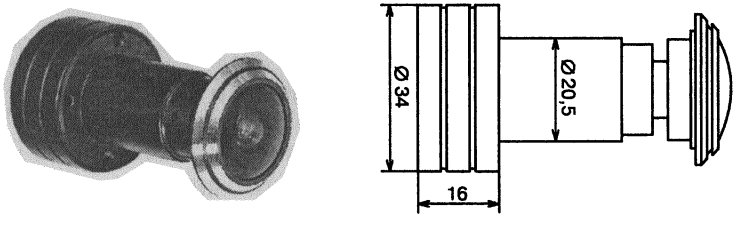


Рис. 1.11. Внешний вид видеоглазка

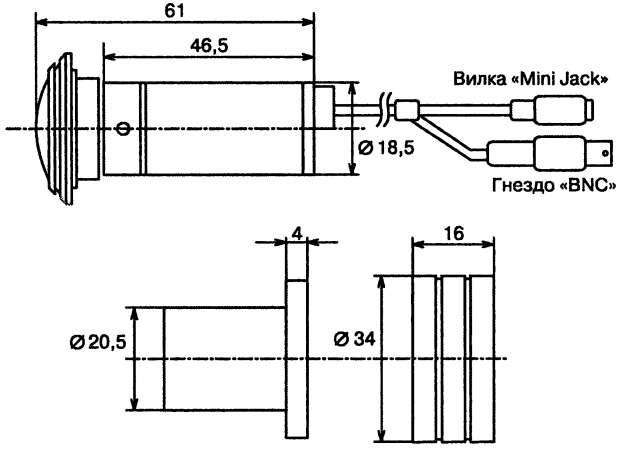


Рис. 1.12. Установочные размеры и выводы для подключения видеоглазка

ного угла зрения, в подобном видеоглазке достаточно просто визуально распознавался объектив телекамеры.

Видеоглазки могут иметь различные **функции и характеристики.**

Цветные видеоглазки. Дают красивую и полную картинку. Но минусом можно назвать слабую чувствительность при плохом освещении. Если у вас на площадке перед дверью постоянно разбивают или воруют лампочки, то цветному видеоглазку лучше предпочесть черно-белый.

Черно-белые видеоглазки. Имеют высокую чувствительность при слабом освещении. А также позволяют использовать инфракрасную подсветку. Инфракрасная подсветка не видна глазу, и может быть выполнена, например, в виде таблички с номером квартиры.

Детектор движения и запись. Современные видеоглазки могут иметь устройство для записи событий при срабатывании встроенного датчика движения. Объем памяти позволяет записать до 32 часов видео.

Аудио запись. Обычно современные модели глазков позволяют, кроме видео записывать и звук.

Монитор. Как правило, видеоглазки с устройством для записи оборудованы ЖК-монитором. Монитор и глазок могут быть выполнены как в виде моноблока, так и отдельных частей. Монитор очень удобен для детей и людей со слабым зрением.

Корпусные и бескорпусные видеоглазки. Корпусные глазки устанавливают на двери, выходящие непосредственно на улицу, для нормальной эксплуатации глазка должна быть обеспечена теплоизоляция.

Автономные. Видеоглазок может быть оборудован аккумуляторной батареей, которая позволяет работать долгое время при отключении электроэнергии.

Беспроводные видеоглазки. Если вы не хотите тянуть провода по квартире, то можно установить беспроводную систему.

Рассмотрим несколько вариантов современных видеоглазков.

Falcon Eye FE-VE01. Дверной видеоглазок FalconEye FE-VE01 (**рис. 1.13, *а***) позволяет осуществлять дистанционное наблюдение за обстановкой перед входной дверью, а также контролировать, что происходит около входной двери в отсутствие хозяев. Датчик движения включает **режим фото и видеозаписи**, записанные файлы хранятся на внешней памяти Micro SD и могут быть в дальнейшем просмотрены.

С внешней стороны двери видеоглазок FalconEye FE-VE01 не отличается от обычного дверного глазка и не привлекает к себе внимания.

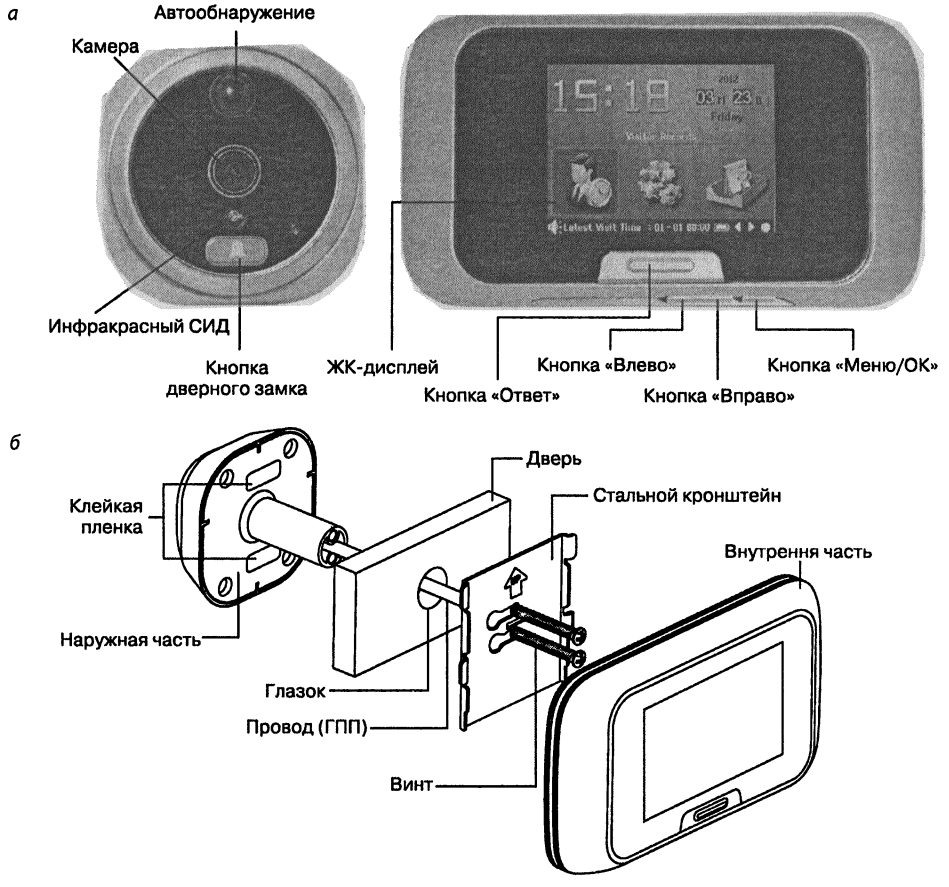


Рис. 1.13. *Видеоглазок Falcon Eye FE-VE01:*
а — внешний вид и органы управления; б — схема сборки

Видеоглазок FalconEye FE-VE01 имеет цветной дисплей 2,8″, русифицированное меню. Предусматривается быстрая несложная установка (**рис. 1.13, *б***).

Функции: скрытое видеонаблюдение и контроль ситуации перед входной дверью. Функция звонка, детектор движения, фото и видеозапись при звонке снаружи или срабатывании детектора движения.

Основные характеристики:

- размеры, мм ..... 136×75×18 (внутри), 60×60×15,5 (снаружи);
- дисплей ..... 2,8″ TFT, QVGA;
- процессор ..... ARM, 104 МГц;
- память ..... 32 Мбит ROM, 32 Мбит RAM;
- внешняя память ..... Micro SD;

- камера ..... QVGA, OV7225;
- ИК подсветка ..... есть;
- питание ..... 3 × AA (алкалиновые батареи);
- в режиме ожидания .. 3—6 месяцев (в зависимости от батарей);
- язык ..... русский, английский;
- настройки ..... установки даты, установки времени, режим ожидания, громкость, выбор звонка, выбор режима записи;
- разрешение (фотозапись) ..... QVGA, 320 × 240;
- автозапись фото ..... при звонке снаружи, при срабатывании детектора движения;
- формат (видеозапись) ..... AVI;
- разрешение (видеозапись) ..... QVGA 320 × 240;
- автоматическая запись видео ..... при звонке снаружи, при срабатывании детектора движения;
- угол обзора камеры ..... 165°.

Дверной глазок черно-белого изображения KPC-190DV (рис. 1.14) — это телекамера с оптической насадкой, расположенная на месте обыкновенного глазка. Видеоглазок устанавливается на месте обыкновенного глазка, внутри двери и снаружи не отличим от стандартного оптического глазка. Видеоглазок в комплекте с монитором представляет собой, по сути, телевизионную систему скрытого наблюдения.

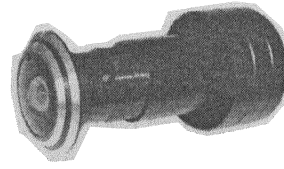


***Рис. 1.14.** Внешний вид видеоглазка KPC-190DV*

Насадка служит для расширения поля зрения камеры (до 120° или 170°) и для маскировки системы под обычный глазок. Монитор предназначен для просмотра изображения и для подачи на камеру напряжения питания 12 В.

Монитор соединяется с камерой кабелем, состоящим из двух проводов питания и одного коаксиального кабеля для передачи видеосигнала (**рис. 1.15**).

Это интересно знать.

Возможно дополнительное удешевление системы за счет отказа от использования монитора. В этом случае видеосигнал подается на линейный НЧ-вход обычного телевизора с низкочастотным входом, а телекамера запитывается от дополнительного источника питания.

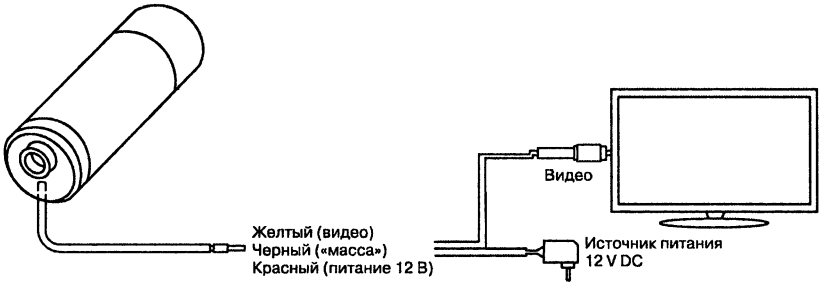


Рис. 1.15. Схема включения видеоглазка KPC-190DV

Основные характеристики:

- производитель ..... КТ&С;
- разрешение ..... 420 ТВ лин;
- чувствительность ..... 0,1 лк;
- ПЗС матрица ..... 1/3 (CCD-SONY);
- угол обзора ..... 176°;
- ток потребления ..... 0,1 А;
- питание ..... 12 В;
- рабочая температура ..... -20...+50 °С;
- габаритные размеры ..... Ø19×5...70 мм.

Видеоглазки обеспечивают хорошее изображение на мониторе при условии определенного уровня освещенности перед дверью. Однако бывают ситуации, когда необходимо наблюдение в полной темноте. Для этого существуют устройства **инфракрасной (ИК) подсветки**.

Невидимое человеком ИК-излучение, тем не менее, хорошо воспринимается видеоглазком. Таким образом, человек, стоящий перед дверью в полной темноте, не будет знать, что за ним осуществляется телевизионное наблюдение.

В комплекте с видеоглазком можно использовать **ИК-пластину**, которая устанавливается на дверь в виде основания квартирного номера. В этом случае пластина крепится над видеоглазком, а на нее наклеиваются цифры квартирного номера.

Это интересно знать.
Для ИК-пластины нужен стабилизированный источник питания 12 В.

Производитель: КТ&С. Данная модель снята с производства.

Дверной глазок черно-белого изображения SK-2019 C (рис. 1.16) имеет цилиндрическую форму. Благодаря этому видеоглазок легко устанавливается в стандартные деревянные и металлические двери толщиной от 33 до 58 мм.

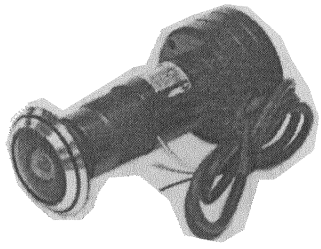


Рис. 1.16. Внешний вид видеоглазка SK-2019 C

Крепление в двери видеоглазка осуществляется с помощью спецгайки, накручиваемой на цилиндрический корпус видеоглазка, имеющего резьбу на своей поверхности. Установка видеоглазка проста и мы рекомендуем ее для самостоятельной установки.

Отличительные особенности: маленький диаметр цилиндрического корпуса; высокая чувствительность и разрешение; простота монтажа; широкий диапазон толщин дверей, используемых для установки видеоглазка.

Основные характеристики:

- производитель.....SUNKWANG;
- разрешение..... 420 ТВЛ;
- чувствительность .....0,1 лк;
- ПЗС матрица ..... 1/3 (CCD-SONY);
- угол обзора..... 176°;
- ток потребления ..... 0,1 А;
- питание ..... 12 В;
- рабочая температура ..... -20...+50 °С;
- габаритные размеры ..... Ø19×5...70 мм

Производитель: Sunkwang (Корея). Данная модель снята с производства.

Варианты установки видеоглазков на базе **бескорпусной монохромной видеокамеры** представлены на **рис. 1.17** и **1.18.**

На **рис. 1.17** показана установка в пустотелую металлическую дверь.

Достоинства: низкая стоимость; малая длина, позволяющая смонтировать видеоглазок в типовую дверь без выступающих элементов.

Недостатки: необходимость довольно большого отверстия в двери обусловленная; поперечными размерами телекамеры (от 44×44 мм до 28×28 мм).

На **рис. 1.18** показана установка видеоглазка **с корпусной монохромной видеокамерой** в сплошную деревянную дверь.

Достоинства: хорошая защита от возможных повреждений при монтаже; приемлемая теплоизоляция при установке в уличные двери.

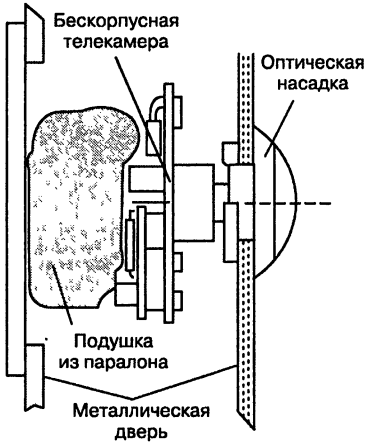


Рис. 1.17. Установка видеоглазка с корпусной моноплатной видеокамерой в пустотелую металлическую дверь

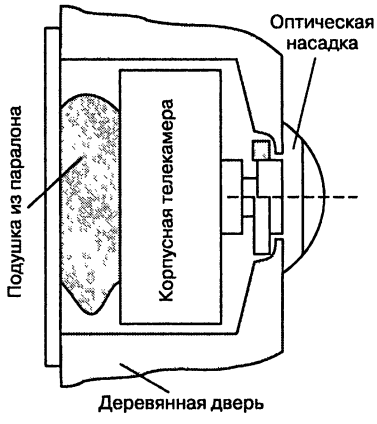


Рис. 1.18. Установка видеоглазка с корпусной моноплатной видеокамерой в сплошную деревянную дверь

Недостатки: несколько большие размеры и стоимость.

В настоящее время разработаны **афокальные оптические насадки** на объектив видеокамеры, обеспечивающие наблюдение в углах зрения до 180° по горизонтали, а по внешнему виду практически идентичные обычным дверным глазкам. С помощью подобных насадок практически любая бескорпусная или малогабаритная корпусная видеокамера со встроенным объективом может быть превращена в видеоглазок. Практически определились две группы видеоглазков — большого (160—180°) и среднего (120—90°) угла зрения. В соответствии с этим подбирается комбинация объектива телекамеры и оптической насадки.

Схема передачи информации от видеоглазка к монитору может быть организована двумя способами:

- передача сигналов изображения происходит по радиоканалу в дециметровом (ДМВ) диапазоне волн на частотах 38—42 телевизионных каналов, для преобразования видеосигнала в радиочастотный ТВ сигнал применяется передатчик телевизионных сигналов;
- передача сигналов изображения по кабелю на НЧ вход телевизора или монитора.

Одной из основных характеристик видеоглазков является **чувствительность**, то есть способность видеоглазка видеть при пониженной освещенности. Чувствительность видеоглазка зависит от характеристики ПЗС матрицы и от светосилы объектива, и измеряется в люксах.

Это интересно знать.
Чем ниже значение этой чувствительности, тем лучше видеоглазок видит при пониженной освещенности.

Все современные видеоглазки чувствительны **в инфракрасной области** спектра и поэтому, при использовании инфракрасной подсветки могут «видеть» даже в полной темноте.

Видеоглазок имеет стандартный **видеовыход** и стыкуется с любым телевизором через НЧ-вход, но для этого ему требуется дополнительный источник питания. Чтобы просматривать изображение с камеры, лучше использовать видеомонитор, т. к. монитор, в отличие от телевизора, имеет высокую четкость (до 1000 линий) и повышенный ресурс работы.

Все многообразие предлагаемых в настоящее время видеоглазков можно разделить на несколько групп, отличающихся техническими параметрами и стоимостью. Для наиболее распространенных моделей характерно применение ПЗС-телекамер со встроенным объективом f = 6 или 3,6 мм и афокальной насадкой. Комбинации различных объективов и насадок позволяют обеспечить углы зрения по горизонтали/вертикали 90/67, 120/ 90 или 170/120°.

Современные дверные видеоглазки имеют различную конструкцию и предназначены для установки на дверях различного типа. Размещение видеоглазка на металлической двери производится аналогично установке обычного дверного глазка.

Благодаря своей цилиндрической форме современный видеоглазок легко устанавливается в стандартные деревянные и металлические двери. Крепление видеоглазка в дверь осуществляется с помощью спецгайки, которая накручивается на цилиндрический корпус видеоглазка, имеющего резьбу на поверхности корпуса.

На **рис. 1.19** показано крепление видеоглазка **с цилиндрической телекамерой** в сплошную деревянную дверь с помощью наружной гайки, на **рис. 1.20** показано крепление видеоглазка в металлическую пустотелую дверь с помощью крышки с упорными кольцами.

Достоинства: удобство и быстрота монтажа.

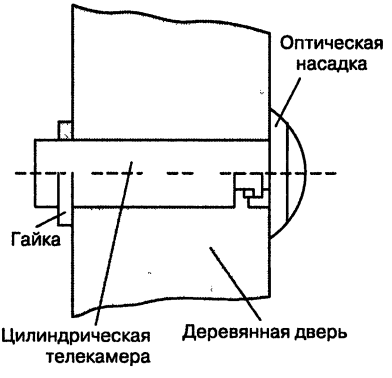


Рис. 1.19. *Крепление видеоглазка в сплошную деревянную дверь с помощью наружной гайки*

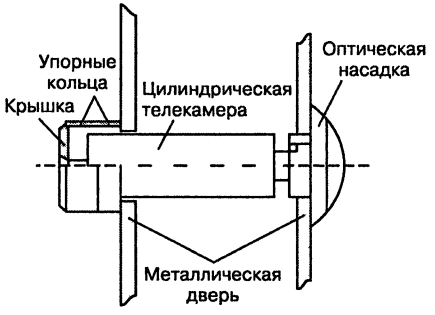


Рис. 1.20. Крепление видеоглазка в металлическую пустотелую дверь с помощью крышки с упорными кольцами

Недостатки: в результате большой длины видеокамеры ее задняя часть выступает из двери; еще большая стоимость, обусловленная более сложной конструкцией камеры и насадки.

Особенности скрытого видеонаблюдения в квартире

Скрытое наблюдение в квартире используется для самых разнообразных целей, например, как средство для контроля над домработницами, нянями, домашним персоналом. Камеры зафиксируют кражу собственности, порчу имущества, иные незаконные действия. Скрытое видеонаблюдение в квартире на сегодняшний день является наиболее эффективным средством опознания при возможном проникновении злоумышленников, вне зависимости от целей, которые они преследуют.

Особенности системы скрытого видеонаблюдения:

- негласное получение и документирование визуальной информации;
- устойчивость к вандализму;
- устойчивость к атмосферным явлениям;
- отсутствие видимых элементов, незаметная камера не портит дизайн.

Системы скрытого видеонаблюдения над квартирой имеют множество **преимуществ**. В первую очередь, они удобны и надежны. Постороннему человеку заметить скрытую камеру невозможно, поэтому исключена вероятность того, что злоумышленник, заметивший камеру, разобьет ее или закроет.

Установка скрытых камер в квартире может преследовать разные **цели**:

- видеонаблюдение за няней;
- видеонаблюдение за прислугой;
- видеонаблюдение за детьми;
- видеонаблюдение за пожилыми людьми;
- видеонаблюдение за больными;
- видеонаблюдение для охраны квартиры.

Особенно это касается няни, ведь ей родители доверяют жизнь собственного ребенка, а сертификаты и дипломы далеко не всегда могут отражать подлинную компетентность няни. При использовании скрытой камеры ребенку будет гарантирована безопасность и родители смогут почувствовать себя намного спокойнее.

Достоинства и недостатки скрытых видеокамер

Достоинства использования скрытых видеокамер:

- камера полностью защищена от вандализма (даже специальные камеры в сверхпрочном корпусе не способны порой справиться с данной задачей);
- злоумышленник в квартире ведет себя развязно, не скрывая своего лица;
- злоумышленник не может вычислить зону охвата камеры;
- существует возможность установки скрытого микрофона неподалеку от камеры.

Недостатки использования скрытых видеокамер:

- стоимость монтажа системы несколько выше;
- на установку скрытых камер требуется достаточно много времени (в среднем от одного до шести часов на одно устройство);
- замена и обслуживание камеры трудоемки (не исключена порча интерьера, и, соответственно, ремонтные восстановительные работы);
- качество изображения со скрытой камеры по сравнению с обыкновенной видеокамерой ниже процентов на десять.

Как правильно установить элементы скрытого видеонаблюдения

В основе практически любой системы видеонаблюдения лежат видеокамера, микрофон, видеорегистратор, монитор.

Если правильно замаскировать системы скрытого видеонаблюдения, то при демонтаже их будет сложно найти. Это справедливо и для профессиональных установщиков, а потому они запоминают расположение камеры относительно соседних объектов.

Миникамеры могут быть спрятаны в датчиках движения (**рис. 1.21**), датчиках пожарной охраны (**рис. 1.22**) или других пассивных инфракрасных датчиках.

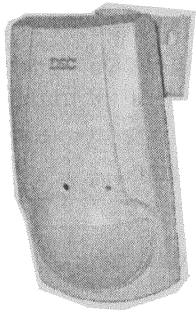


Рис. 1.21. Миникамера, установленная в датчике движения

Это идеальный вариант для новичков. Для большинства людей они будут незаметны. Чаще всего в них устанавливают камеры типа «board» или « pin-hole» обладающие фокусным расстоянием на 3,6 мм.

Будьте осторожны.
Некоторые видеокамеры могут перегреваться, особенно если установить камеру на пластиковую или деревянную поверхность.

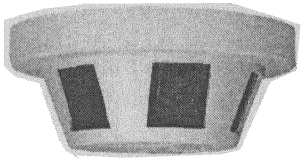


Рис. 1.22. Миникамера, установленная в датчике пожарной охраны

Миниатюрные видеокамеры можно встроить в предметы интерьера. Устройства, оборудованные вынесенным зрачком входа, позволяют оставить снаружи едва заметное отверстие объектива величиной со спичечную головку. Заметить такую видеокамеру можно разве что с использованием специальной техники.

Очень часто видеокамеры прячут в листьевых растениях и в цветах. Такого рода установка не требует больших усилий и в любой момент можно переместить или извлечь камеру.

Отличные места для скрытых камер — розетки, люстры, выключатели. Кроме того, камеры прячут в бытовую технику, в мягкие или пластиковые игрушки. Хотя последнее запрещено законодательно и предусматривает уголовную ответственность.

Встраивание камер в стенку, карниз или потолок — трудоемкий, но самый надежный вариант. Монтаж такого типа предполагает также прокладку кабеля внутри стены или под потолком.

Приняв решение о монтаже охранной видеосистемы, необходимо сразу же подумать о том, куда спрятать устройство записи. Оптимальным вариантом для скрытой записи, кстати сказать, станет **видеорегистратор**. Лучше всего разместить видеорегистратор в тайнике, и здесь уже все зависит от мастерства и фантазии человека, занимающегося монтажом. Часто устройства записи размещают в скрытых стенных нишах, над подвесными потолками, под полом или даже на лоджии, при условии, что она утеплена.

Совет.
Специалисты рекомендуют использовать скрытые видеокамеры с датчиками движения, имеющие небольшие размеры, но серьезные технические характеристики.

Сегодня особенно популярны **беспроводные миникамеры с датчиком движения**, имеющие в основе видеорегистратор. Любая разновидность системы скрытого видеонаблюдения имеет свои плюсы и свои минусы, поэтому подбирать ее следует исходя из поставленных задач и с учетом индивидуальной ситуации.

Скрытое видеонаблюдение в темноте

Микрокамеры скрытого видеонаблюдения не могут производить наблюдение и съемку в темное время суток, а ведь камера должна записывать все время и особенно ночью.

Эту проблему решает **инфракрасная подсветка**. Свет от ИК-подсветки не виден человеческому глазу, но матрица цифровой камеры его определяет.

ИК-подсветку тоже надо хитро спрятать в интерьере. В продаже имеется готовая ИК-подсветка для систем скрытого видеонаблюдения в форме:

- **болта** — дальность освещения 1—1,5 м, при близком расстоянии легко распознать (**рис. 1.23**);
- шпильки — дальность освещения 1,5—2 м (**рис. 1.24**);
- **номера от квартиры** — дальность освещения 3 м (**рис. 1.25**);
- **обычного выключателя** — дальность освещения 5 м;

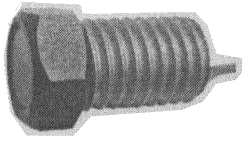


Рис. 1.23.

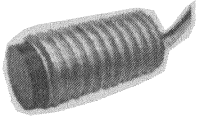


Рис. 1.24.

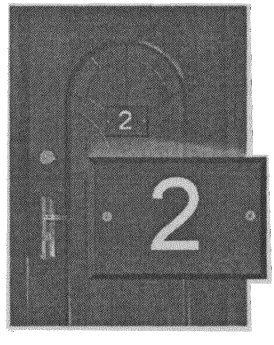


Рис. 1.25.

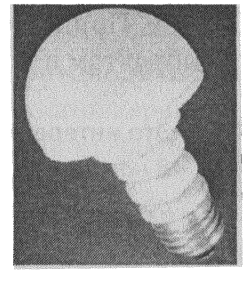


Рис. 1.26.

- **«неработающей» лампочки** (ИК-лампы, **рис. 1.26**), которая может осветить наибольшую площадь до 40 м^2;
- **специального прожектора.** Например, Viatec S12D-IR (**рис. 1.27**). Цвет корпуса: серый. Установка: наружная. Дальность подсветки до: 210. Угол подсветки: 30 градусов. Количество ИК-диодов: 12. Напряжение питания: 110—220 В.

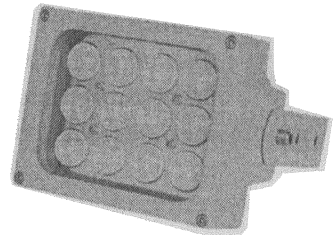


Рис. 1.27.

Полезные советы по установке скрытого наблюдения

Установка скрытого наблюдения является нестандартным творческим процессом, который требует терпеливости, аккуратности и определенных профессиональных знаний и навыков, которые знают, как установить скрытое видеонаблюдение. Для достижения эффективности работы системы необходимо учесть **советы** и **правила** установки видеонаблюдения.

Совет 1. Выбирайте оптимальный размер камеры для качественной маскировки, поэтому используйте миниатюрные видеокамеры.

Совет 2. Установить камеры следует таким образом, чтобы обеспечить наибольший радиус обзора.

Совет 3. Провода питания и все элементы системы надежно скройте.

Совет 4. Помните, что маскировочная отделка видеокамеры должна быть пожароустойчивой, ведь при работе видеокамера нагревается.

Совет 5. Обеспечьте хорошую маскировку не только камеры, но и видеорегистратора, который должен быть без встроенных вентиляторов охлаждения, чтобы избежать шумового фона.

Совет 6. При использовании инфракрасной подсветки для слежения за объектом в темноте необходимо спрятать и сам прожектор.

Это интересно знать.

В настоящее время разработаны готовые устройства с вмонтированными в них ИК-осветителями, похожие на различные предметы (выключатель, лампочка, болт).

Самостоятельная установка системы скрытого видеонаблюдения

Перед монтажом системы видеонаблюдения в квартире стоит определить, что именно является объектом наблюдения: входная дверь, лестничная площадка, спальня, гостиная, детская комната, окна и пр. Пример наполнения системы видеонаблюдения в квартире представлен на **рис. 1.28.**

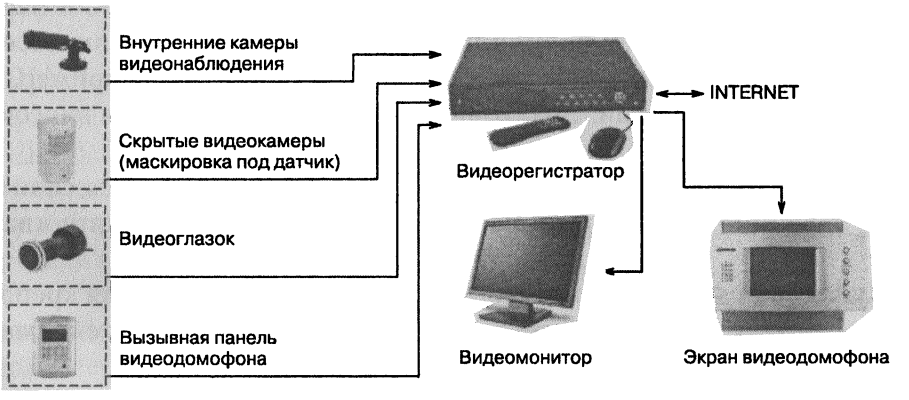


Рис. 1.28. *Пример наполнения системы видеонаблюдения в квартире*

Далее необходимо составить четкий план точек, с которых будет вестись наблюдение. Затем следует приобрести необходимые компоненты системы. Если планируется оборудовать **беспроводную систему наблюдения**, то необходимость в прокладке кабелей отсутствует.

Это интересно знать.
Использование беспроводных видеокамер не всегда дает желаемый эффект. Это объясняется тем, что батарейки камер имеют ограниченный ресурс, сами камеры обладают небольшим радиусом действия и недостаточным качеством изображения.

При подготовке плана прокладки кабелей производится расчет расстояния до каждой камеры. Можно сделать простой карандашный рисунок с указанием всех данных. Если расстояние между камерами меньше 30 м, то для квартиры достаточно 4 камер.

Прокладка кабелей во время ремонтных или строительных работ в жилом помещении не представляет никаких сложностей. Для этого есть несколько эффективных методов: штробление, укладка кабеля под заливными полами или за натяжными/подвесными потолками.

Совет.

Если же ремонтные работы завершены, то специалисты рекомендуют использовать ***ШСМ-провод*** *(комбинированный многожильный) толщиной 3×4 мм. Его прокладывают в дверных косяках, внутри или позади плинтуса.*

Человек, решивший установить систему видеонаблюдения, должен обращать особое внимание на такой важнейший технический параметр видеокамеры как **возможность при изменении уровня освещения** переходить из одного режима съемки в другой. Например, из цветного в черно-белый. Такого эффекта позволяет добиться видеокамера с инфракрасной подсветкой и датчиком движения.

Существует несколько видов камер, которые различаются своими спецификациями, которые выбрать для видеонаблюдения в квартире.

Купольные камеры. Они выполняются в форме купола для крепления к потолку. Есть модификации таких устройств с кронштейнами и сложными поворотными трансфокаторами.

Модульные камеры. Это устройства начального уровня, которые отличаются доступностью в цене и удобством для скрытого наблюдения.

Корпусные камеры. Они чаще всего рекомендуются для самостоятельной организации видеонаблюдения в жилых помещениях. Такие камеры позволяют достичь наиболее качественного изображения.

Изображение, поступающее с видеокамер, может быть передано практически на любое расстояние. Монтаж системы осуществляют профессионалы, умеющие замаскировать камеру таким образом, что догадаться о ее наличии в квартире абсолютно невозможно.

Рынок предлагает большой ассортимент всевозможных скрытых видеокамер. Например, **мини-камеры с датчиками звука.** Запись на мини-камеру начинается после того, как в помещении раздался какой-то шум. Мини-камера очень компактна, ее несложно замаскировать. Производители комплектуют устройство различными крепежными приспособлениями: шурупы, клипсы, двусторонняя лента. Встроенная батарейка позволяет камере записывать видео в формате **avi** до двух часов.

После выбора оптимальных устройств скрытого видеонаблюдения и кабелей производится **монтаж** и подключение по подготовленному заранее плану и схеме подключения.

Установка элементов системы видеонаблюдения содержит следующие шаги.

Шаг 1. Установка видеокамер в заранее выбранные места.

Шаг 2. Подключение соединительных кабелей к видеорегистратору.

Шаг 3. Подключение видеокамер к соединительному кабелю.

Шаг 4. Подключение видеокамер к блоку питания с соблюдением полярности: черные провода подключаются к черным, красные — к красным.

Шаг 5. Подключение монитора или телевизора к видеорегистратору.

Шаг 6. Подключение видеорегистратора к сети.

Чтобы подключить камеры к монитору и записывающему устройству используют коаксиальный кабель. Основная задача кабеля — передача видеосигнала к принимающему устройству.

Качественный кабель обеспечит передачу видео без потерь на расстояние до трехсот метров от камеры. Это следует учитывать, если в доме несколько этажей или камеру планируется использовать для наружного видеонаблюдения.

Очень важный момент — **настойка электропитания**. Некоторые камеры обладают специальным режимом автономного питания.

Затем следует приступить к настройке камер. Лучше всего для этой цели применить портативный монитор и провод с соединительными разъемами, которые подходят для подготовленного монитора. Это позволит максимально комфортно настроить требуемый угол обзора и резкость объектива камеры.

При самостоятельном монтаже системы видеонаблюдения необходимо учитывать, что в данном процессе должны быть задействованы как минимум два человека. Например, на этапе настройки камеры один человек выбирает верный радиус обзора, а второй следит за полученным на дисплей изображением.

Установка скрытых камер в квартире — процесс достаточно сложный.

Часто камеры размещают прямо в стене, для этого в ней делается сквозное углубление. В это место добавляют раствор и вставляют камеру. После этого камеру следует подключить к монитору и настроить. Глазок должен находиться в одной плоскости со стенной поверхностью. Когда верный угол обзора выбран, можно начинать процесс окончательного закрепления. В отверстие добавляют немного раствора. Крайне важно не смещать камеру, иначе придется вновь про-

изводить ее настройку. Когда производится замазка отверстия, глазок должен быть чем-то закрыт, чтобы на объектив не попал раствор.

Для полной маскировки видеокамеры, поверхность следует закрасить краской того же тона, что и стена. Покраску производят после того, как раствор окончательно засох.

Видеорегистратор. Чтобы организовать качественное скрытое видеонаблюдение в квартире, необходимо подобрать оптимальный видеорегистратор с нужной функциональностью. При выборе стоит обратить внимание на следующие характеристики:

- количество аудио- и видеоканалов (при установке 4 камер каналов должно быть четыре и больше);
- скорость записи. При формате записи 360×288 с четырьмя камерами обеспечивается оптимальная скорость в 25 кадров в секунду;
- формат записи.

Это интересно знать.

Для установки сетевого клиента и просмотра через интернет требуются специальные навыки и знания. Поэтому для организации такой функциональности стоит обратиться к опытным специалистам и компаниям.

Установка системы скрытого наблюдения с использованием технологии Wi-Fi

Это интересно знать.

***Wi-Fi** (от англ. Wireless Fidelity) — это торговая марка беспроводных сетей, построенных на базе стандарта IEEE 802.11. Дословно переводится как «высокая точность беспроводных сетей». Любое оборудование стандарта IEEE 802.11 может получить сертификат ношения логотипа Wi-Fi, при прохождении соответствующего тестирования.*

Главным преимущество данной технологи является отсутствие проводов, что позволяет сократить время установки всей системы. Тем более это все можно будет установить в местах, где прокладка кабеля вообще невозможна. Единственное, нужно будет обеспечить питанием каждую из камер.

Огромный плюс использования Wi-Fi в вашей системе безопасности заключается в большом радиусе действия. Обычно даже стены не

мешают передачи сигнала, но при их отсутствии и наличии прямой видимости радиус стандарта Wi-Fi может достигать 500 м.

Существуют также несколько типов антенн, которые могут существенно увеличить расстояние. Данные с записывающих устройств не сохраняются в памяти самой камеры, а тут же передаются на видеосервер, которым обычно служит ноутбук или стационарный компьютер.

Камеры являются сетевыми устройствами, при этом имеют свой выделенный IP адрес. Данными с камер можно управлять: удалять, сохранять, сжимать и т. д.

Глушение сигнала в беспроводной сети возможно. Но чтобы этого достичь, нужен очень мощный источник, который смог бы полностью заглушить передачу данных. А также он должен располагаться в непосредственной близости от видеокамер.

Повысить помехоустойчивость беспроводной сети можно с помощью специальных узконаправленных антенн.

Желательно поддерживание Wi-Fi камерами **стандартных алгоритмов сжатия изображения**, чтобы можно было передать данные высокого качества.

Сфера применения Wi-Fi видеонаблюдения очень велика. Начиная от построения систем безопасности в огромных офисах, и заканчивая небольшими загородными домами. Wi-Fi видеонаблюдение становится полностью надежным и удобным средством обеспечения безопасности в вашем помещении.

Установка скрытых камер видеонаблюдения без проводов

Мини камеры наблюдения передают сигнал на определенном расстоянии с помощью проводов или радиоволн. В большинстве случаев популярностью пользуются беспроводные скрытые камеры видеонаблюдения. Они обладают хорошей мобильностью и дают лучший эффект. Минимизация камер вызвана не столь большим желанием использовать их в качестве шпионских, для получения незаконной информации.

Дело в том, что камеры наружного наблюдения вызывают у людей некоторую агрессию и привлекают лишнее внимание. Поэтому сейчас для установки скрытых камер видеонаблюдения используют мини или даже микро видео камеры. Они устанавливаются в стенах и маскируются в различных декоративных элементах интерьера комнаты. В тех случаях, когда помещение оборудовано датчиками пожарной безопасности, то установку камер производят именно в них.

Еще одним преимуществом установки беспроводных скрытых камер видеонаблюдения является и ничтожное потребление электроэнергии. При монтаже камеры необходимо подумать и об обеспечении освещения в темное время суток. Как правило, большинство современных компаний производят камеры со встроенным инфракрасным освещением. Это вызвано тем, что камеры используются для скрытого видеонаблюдения, а как известно инфракрасный свет не видим человеческому глазу, но при этом дает достаточно освещенности для цифровой видеокамеры. Устанавливая мини или микровидеокамеру в стене нужно учитывать и тот факт, что демонтаж ее будет затруднен, поэтому при установке стоит направлять объектив камеры как можно точно именно в ту сторону, где расположен участок наблюдения.

Многие беспроводные скрытые камеры видеонаблюдения обладают ограниченным радиусом передачи сигнала. Для таких случаев существуют специальные усилители радиосигнала. Они значительно увеличивают дальность передачи изображения, но стоит учитывать, что для каждой модификации камер видеонаблюдения необходимо подбирать и соответствующий усилительный прибор.

1.3. Видеонаблюдение в частных домах

Видеонаблюдение в частных домах имеет серьезные отличия от видеонаблюдения в квартирах. Связано это с тем, что в частных домах съемка чаще ведется на улице, т. к. необходимо получить видеоинформацию о том, что происходит уже на подступах к дому. Видеообзор периметра дома предполагает использование специальных камер, они не только должны быть защищены влагостойкими и термозащищенными корпусами, они должны иметь широкую амплитуду «рабочих» температур — тех температур, при которых их работа будет вестись в нормальном режиме.

Это интересно знать.
Камеры, работающие на улице, как правило, имеют отличные от «домашних» камер разрешающие способности объектива и матрицы.

При хорошем дневном освещении получить качественную картинку не сложно даже с использованием не дорогой камеры. А как

получить максимально широкий угол обзора, как добиться качественной съемки при недостаточном освещении?

Проектирование системы видеонаблюдение для коттеджа — задача серьезная, требующая специальных навыков, поэтому доверять ее надо профессионалам. Если вы хотите иметь картинку всего периметра, камеры должны располагаться так, чтобы между ними не было «мертвых» зон. Но также важно и не переборщить с количеством камер. Да, большое количество телекамер обычно выглядит впечатляюще. Однако необходимо серьезно оценить, какое влияние это окажет на работу всей системы видеонаблюдения. Ведь зачастую можно меньшим количеством камер иметь тот же самый обзор, что и большим количеством, главное правильно их разместить.

Особое внимание нужно уделять монтажу камер. Они могут монтироваться как на потолочном, так и на настенном кронштейне. Сам кронштейн может быть как фиксированным, так и подвижным — на поворотной платформе, что дает — при наличии дополнительного оборудования — возможность дистанционно управлять камерой, повышая зону охвата.

Видеонаблюдение дома используется для защиты и контроля доступа. Часто используется связка **видеонаблюдение + сигнализация + домофон**, т. е. совместно с системой видеонаблюдения используется система сигнализации и домофон. Такая система позволяет контролировать внутренние помещения, улицу и периметр, а в случае попытки проникновения активировать сирену, отправить «тревожное сообщение» на сотовый телефон, сообщить в пункт централизованного наблюдения.

На вход обычно устанавливается видеодомофон. При обширной территории желательно использовать беспроводные видеокамеры. При необходимости устанавливаются датчики движения. Можно использовать поворотные устройства для сокращения числа видеокамер.

Комплексная система решает такие задачи:

- видеонаблюдение подконтрольной территории (полный обзор внутренних помещений, дверей, территории внутри забора, вход и въезд на территорию участка, периметр);
- видеозапись длительностью до нескольких недель;
- хороший обзор в условиях пониженной видимости (ночью);
- запись по тревоге;
- отправка голосовых или текстовых сообщений на телефон при возникновении «тревожной ситуации».

На улице должны использоваться видеокамеры с герметическими кожухами. В условиях пониженной видимости должны использоваться камеры с ИК прожекторами. Излучение не видно глазу и, в то же время хорошо, освещает объект. ИК прожектор может быть встроен в видеокамеру (в вызывной панели видеодомофона). Желательно цифровое улучшение изображения в условиях плохой видимости.

При обширности наблюдаемой территории рекомендуется использовать беспроводное видеонаблюдение. В этом случае снижаются затраты на прокладку кабеля. При использовании беспроводных камер очень легко поменять расположение камер в случае проведения каких-либо работ на подконтрольной территории.

Удобно с видеосистемой устанавливать датчики движения для фиксации перемещения в области видимости камеры и для принятия необходимых мер.

Совет.

Для экономии места на жестком диске можно использовать режим «запись по тревоге», т. е. система начинает записывать видеоинформацию при возникновении нештатной ситуации.

1.4. Видеокамеры для скрытого наблюдения

Цветные видеокамеры для скрытого наблюдения

Цветная видеокамера для скрытого наблюдения в квадратном миникорпусе KPC-S700CP4-4,3 (рис. 1.29) предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта.

- Размер матрицы ..... 1/3″.
- Наличие объектива ..... да.
- Тип камеры ..... миниатюрная квадратная.
- Изображение ..... цветное.
- Климатическое исполнение ..... внутреннее.
- Вандалозащищенность ..... нет.
- Напряжение питания ..... 12.

Особенности: квадратный миникорпус, цветная, 30×30 мм; SONY 1/3″ CCD; 380 ТВЛ; 1 Лк/F2,0; f = 4,3 мм; pin-hole (конус); 11—13 В DC/110 мА; AWB; AGC; 30×30×30 мм.

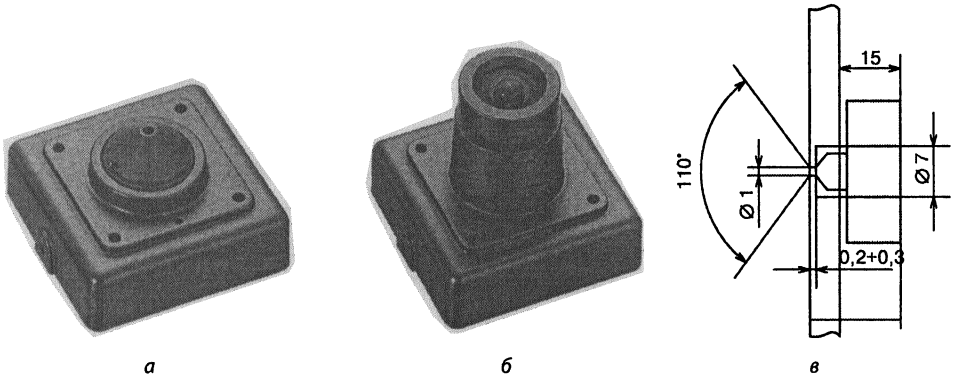


Рис. 1.29. *Видеокамера в квадратном миникорпусе KPC-S700CP4-4,3: а — без оптики; б — с оптикой; в — габаритные размеры и пример установки*

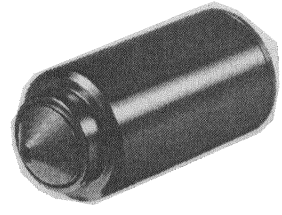


Рис. 1.30. *Внешний вид видеокамеры EN-TBC-32*

Цветная видеокамера для скрытого наблюдения в цилиндрическом миникорпусе EN-TBC-32 предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта.

- Матрица ..... 1/3 SONY.
- Разрешение..... 420 ТВЛ.
- Характеристика изображения..... PAL: 500 (H) × 582 (V). NTSC: 510 (H) × 492 (V).
- Минимально освещение..... 0,8 Lux / F2,0.
- Система цветности..... PAL / NTSC.
- Объектив..... 3,7 мм, конус, «pin-hole»объектив.
- Отношение сигнал / шум ..... более 48 дБ.
- Электронный затвор .... NTSC: 1/60 — 1/100, PAL: 1/50 — 1/110.
- Гамма ..... 0,45.
- Баланс белого.....автоматический.
- Видео выход..... 1 p-p / 75 Ом.
- Электропитание .....DC12 В ± 10%.
- Рабочая температура.....-10 °С ... +50 °С.
- Размеры.....∅22 × 100 (В) мм.
- Вес.....200 г.

Цветная видеокамера для скрытого наблюдения в цилиндрическом миникорпусе KPC-S230CP4-4,3 предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта (**рис. 1.31**).

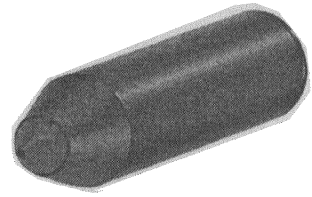


Рис. 1.31. Внешний вид видеокамеры KPC-S230CP4-4,3

- Размер матрицы .....1/3″.
- Наличие объектива ..... да.
- Тип камеры. миниатюрная квадратная.
- Изображение ..... цветное.
- Климатическое исполнение ..... внутреннее.
- Вандалозащищенность ..... нет.
- Напряжение питания .....12.

Особенности: цилиндрическая цветная камера видеонаблюдения. SONY 1/3″ CCD; 380 ТВЛ; 1 Лк/F2,0; f=4,3; d=23 мм, AWB; AGC; конус; DC 11—13 В / 110 мА.

Рис. 1.32. Внешний вид видеокамеры KPC-S230CP4-78 (4,3)

Цветная видеокамера для скрытого наблюдения в цилиндрическом миникорпусе KPC-S230CP4-78 (4,3) предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта (**рис. 1.32**).

Видеокамера KPC-S230CP4-78 (4,3) — цветная цилиндрическая видеокамера KT&C оснащена матрицей SONY. Невысокая стоимость KPC-S230CP4-78 (4,3) делает ее особенно привлекательной. KPC-S230CP4-78 (4,3) имеет среднее разрешение. Наличие у KPC-S230CP4-78 (4,3) объектива «pin-hole» позволяет осуществить скрытую установку данной видеокамеры. Показатель SN 50 дБ также говорит о хорошем качестве изображения KPC-S230CP4-78 (4,3).

- Стандарт TV-сигнала.....PAL, NTSC.
- ПЗС-матрица.....SONY 1/3″ SUPER HAD CCD.
- Разрешение..... 420 ТВЛ.
- Чувствительность.....0,9 Lux (при относит. отверстии F=2,0).
- Отношение сигнал/шум ..... более 48 дБ.
- Объектив..... f 2,97/3,6/6/8/12 мм.
- Баланс белого..... есть.
- Автоматическая регулировка усиления ..... есть.
- Электронный затвор .....автоматич. 1/50—1/100000 с.
- Напряжение питания .....пост. 9—15 В.
- Рабочая температура .....-10°C...+50°C.

Черно-белые видеокамеры для скрытого наблюдения

Черно-белая скрытая видеокамера в цилиндрическом миникорпусе KPC-S190SP4-4,3 предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта.

Миниатюрная цилиндрическая камера видеонаблюдения KT&C KPC-S190SP4-78 (4,3) с объективом boardlens предназначена для установки в помещениях. Может использоваться как самостоятельное устройство в недорогих системах видеонаблюдения. Внешний вид видеокамеры представлен на **рис. 1.33**. Пример использования камеры в режиме дверного видеоглазка представлен на **рис. 1.34**.

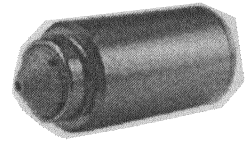


Рис. 1.33. *Внешний вид видеокамеры KPC-S190SP4-4,3*

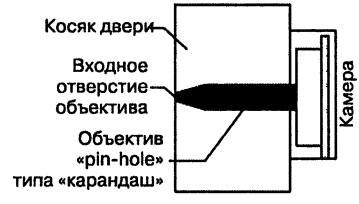


Рис. 1.34. *Пример использования камеры в режиме дверного видеоглазка*

Подключается к любым видеомониторам, видеодомофонам и устройствам обработки видеосигнала (квадратор, мультиплексор, видеомагнитофон). Чувствительность черно-белой камеры KT&C KPC-S190SP4-78 (4,3) расширена в инфракрасную область, что позволяет осуществлять ночное видеонаблюдение с применением инфракрасной подсветки, не воспринимаемой человеческим глазом.

Из-за малых размеров входного зрачка объектива маскировка бескорпусных и миниатюрных телевизионных камер может быть самой различной: в двери, стене, плинтусе, коробе и т. п.

Использование высокочувствительной матрицы компании SONY обеспечивает камере видеонаблюдения высокое разрешение и чувствительность. Камера комплектуется шарнирным кронштейном, что позволяет ориентировать ее в любой плоскости.

- Размер матрицы ..... 1/3″.
- Наличие объектива ..... да.
- Тип камеры..... миниатюрная квадратная.
- Чувствительный элемент ..... ПЗС 1/3″.
- Разрешающая способность, твл ..... 420.
- Чувствительность, лк..... 0,005.
- Синхронизация..... внутренняя.
- Электронная регулировка освещенности ES..... 1/50...1/100000.
- Объектив, вариофокальный f, мм .. 3,7 (pin-hole полный конус).

- Напряжение питания DC, В.....12.
- Потребляемый ток, мА.....100.
- Диапазон рабочих температур, °С.....-10...+50.
- Габаритные размеры, мм.....∅19×41.
- Изображение.....черно-белое.
- Климатическое исполнение.....внутреннее.
- Вандалозащищенность.....нет.
- Напряжение питания.....12.

Особенности: Цилиндрическая черно-белая камера видеонаблюдения стандартного разрешения; SONY 1/3″ CCD; 420 ТВЛ; 0,05 Лк/F2,0; f= 4,3 мм (76'); 9—15 В DC/0,1 А; pin-hole (конус); штатив.

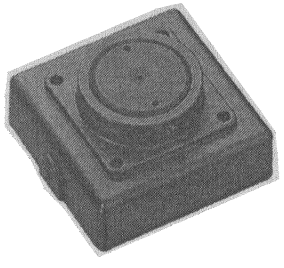


Рис. 1.35. Внешний вид видеокамеры KPC-S400P4-78 (4,3)

Черно-белая скрытая видеокамера в квадратном миникорпусе KPC-S400P4-78 (4,3) предназначена для системы скрытого видеонаблюдения, охраны и контроля объекта (**рис. 1.35**).

Видеокамера KT&C KPC-S400P4-78 (4,3) — черно-белая миниатюрная видеокамера, как и все камеры KT&C, оснащена матрицей SONY. Невысокая стоимость KT&C KPC-S400P4-78 (4,3) обусловлена средним разрешением, что в свою очередь не снижает качество картинки. Безусловный плюс данной видеокамеры в ее миниатюрных размерах. Наличие у KT&C KPC-S400P4-78 (4.3) объектива «pin-hole» позволяет осуществить скрытую установку данной видеокамеры. Показатель SN 50 дБ также говорит о хорошем качестве изображения KT&C KPC-S400P4-78 (4,3). Видеокамера KT&C KPC-S400P4-78 (4,3) также имеет довольно неплохую чувствительность, что также делает ее привлекательной.

- Размер матрицы.....1/3″.
- Наличие объектива.....да.
- Тип камеры.....миниатюрная квадратная.
- Изображение.....черно-белое.
- Климатическое исполнение.....внутреннее.
- Вандалозащищенность.....нет.
- Напряжение питания.....12.

Особенности: SONY 1/3″ CCD; 420 ТВЛ; 0,05 Лк/F2.0; f= 4,3 мм (90'); 9—15 В DC/0,1 А; pin-hole (конус); 30×30×19 мм. Квадратный миникорпус 30 × 30 мм.

1.5. Видеорегистраторы

Видеорегистратор — это устройство для записи, обработки и хранения записи видеосигнала, поступающего с видеокамер, вывода хранимого или обрабатываемого видеосигнала на монитор пользователя.

Это интересно знать.
В настоящее время большинство видеорегистраторов позволяет транслировать сигнал с видеокамер по сети интернет.

Количество каналов. От количества каналов зависит, какое количество камер (4, 8, 16) можно подключить к данному видеорегистратору.

Скорость записи. От скорости записи зависит, какое видео вы получите. Если будет 25 кадров в секунду на канал, то это значит, что вы сможете просматривать видео как обычный фильм. В случае если указано, отличное число от 25 кадров на канал, значит, вы будете видеть прерывистое видео. Т. е. если в кадре идет человек, то вы будете видеть не весь его путь, а отрывками и чем меньше кадров на канал, тем больше будет пробел в отображении видео.

Разрешение записи. От данного параметра, как правило, зависит качество записанного видео, т. е. чем выше разрешение записи, тем лучшее качество картинки.

Это интересно знать.
В аннотации к видеорегистратору указывается, при каком разрешении какая скорость записи.

Например, при разрешении записи 720×576 скорость записи может составлять 6 кадров в секунду на канал, а при разрешении записи 360×288 скорость записи будет 25 кадров в секунду на канал.

Дополнительные функции видеорегистратора. Вышеперечисленные параметры являются основными для выбора видеорегистратора.

Объем жесткого диска определяет, как много информации будет храниться на нем.

Это интересно знать.
*Выбирая жесткий диск необходимо обратить внимание на **формат**, в котором видеорегистратор производит запись, разрешение записи и тип используемых видеокамер.*

Так же на объем жесткого диска будет влиять функция видеорегистратора запись по движению. Данная функция позволяет вести не сплошную запись, а только тех фрагментов, когда в кадре происходит какое-либо движение. На сайтах производителей видеорегистраторов имеется список жестких дисков, с которыми данная модель видеорегистратора тестировалась.

Наличие в видеорегистраторе сетевой платы позволяет производить просмотр записи из любой точки земного шара, где имеется интернет, при условии, что вы его подключите к интернету.

Наличие в видеорегистраторе аудио входа позволит вам производить запись видео со звуком. Количество аудио входов для различных моделей видеорегистраторов различно.

Все чаще стали выпускаться видеорегистраторы, которыми возможно управлять при помощи USB мыши, используемой для компьютера. Видеорегистратор может иметь возможность подключения мыши для управления или комплектоваться ею.

В подавляющем большинстве видеорегистраторы, хоть и хранят информацию на жестком диске, но просмотреть ее напрямую компьютере не возможно. И только малая часть из представленных на рынке видеорегистраторов позволяет подключать жесткий диск к компьютеру и просматривать хранящуюся на нем информацию.

Это интересно знать.
Как правило, такие видеорегистраторы имеют съемный лоток для быстрой замены жесткого диска.

Для отображения видео видеорегистратор может иметь разъем VGA для подключения монитора аналогичному тому, что используется для компьютера и BNC для подключения к телевизору.

ГЛАВА 2

ШПИОНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И БОРЬБА С НИМ

Данная глава посвящена вредоносному программному коду, актуальной в настоящий момент проблеме. Еще недавно ситуация была достаточно простой — существовали прикладные программы и компьютерные вирусы (программы, способные заражать другие приложения путем внедрения в них своего машинного кода). Но последнее время появилось множество вредоносных программ, которые нельзя считать вирусами, т. к. они не обладают способностью к размножению.

1.1. Программные «шпионы»

SpyWare

Для вредоносных программ существует множество категорий: Trojan, **Backdoor**, Trojan-Downloader, MalWare, SpyWare, Adware, **Dialer** и др.

Определение.
Программой-шпионом *(альтернативные названия — Spy, SpyWare, Spy-Ware, Spy Trojan...) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.*

Шпионское ПО применяется для ряда целей, из которых основным являются маркетинговые исследования и целевая реклама. В этом случае информация о конфигурации компьютера пользователя, исполь-

зуемом им программном обеспечении, посещаемых сайтах, статистика запросов к поисковым машинам и статистика вводимых с клавиатуры слов позволяет очень точно определить род деятельности и круг интересов пользователей.

Поэтому чаще всего можно наблюдать связь SpyWare — Adware, т. е. «Шпион» — «Модуль показа рекламы». Шпионская часть собирает информацию о пользователе и передает ее на сервер рекламной фирмы. Там информация анализируется, и в ответ высылается рекламная информация, наиболее подходящая для данного пользователя.

В лучшем случае реклама показывается в отдельных всплывающих окнах, в худшем — внедряется в загружаемые страницы и присылается по электронной почте.

Собранная информация может использоваться не только для рекламных целей. Например, получение информации о ПК пользователя может существенно упростить хакерскую атаку и взлом компьютера пользователя. А если программа периодически обновляет себя через Интернет, то это делает компьютер очень уязвимым — элементарная атака на DNS может подменить адрес источника обновления на адрес сервера хакера — такое «обновление» приведет к внедрению на ПК пользователя любого постороннего программного обеспечения.

Шпионское программное обеспечение может попасть на компьютер пользователя двумя основными путями.

Путь 1. В ходе посещения сайтов Интернет. Наиболее часто проникновение шпионского ПО происходит при посещении пользователем хакерских и warez сайтов, сайтов с бесплатной музыкой и т. д.

Это интересно знать.
Как правило, для установки шпионского ПО применяются ActiveX компоненты или троянские программы категории TrojanDownloader по классификации лаборатории Касперского. Многие хакерские сайты могут выдать «крек», содержащий шпионскую программу или TrojanDownloader для ее загрузки.

Путь 2. В результате установки бесплатных или условно-бесплатных программ.

Это интересно знать.
Множество подобных программ распространяется через Интернет или на пиратских компакт-дисках. Классический при-

мер — кодек DivX, содержащий утилиту для скрытной загрузки и установки SpyWare.Gator.

Будьте осторожны.
Большинство программ, содержащих SpyWare-компоненты, не уведомляют об этом пользователя.

Spyware могут осуществлять широкий круг задач:

- собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);
- запоминать нажатия клавиш на клавиатуре (кейлоггеры) и записывать скриншоты экрана (screen scraper) и в дальнейшем отправлять информацию создателю spyware;
- несанкционированно и удаленно управлять компьютером (remote control software) — бэкдоры, ботнеты, droneware;
- инсталлировать на компьютер пользователя дополнительные программы;
- использоваться для несанкционированного анализа состояния систем безопасности (security analysis software) — сканеры портов и уязвимостей и взломщики паролей;
- изменять параметры операционной системы (system modifying software) — руткиты, перехватчики управления (hijackers) и пр. — результатом чего является снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ;
- перенаправлять активность браузеров, что влечет за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Меры по предотвращению заражения:

- использование браузеров, отличных от Internet Explorer — Opera, Mozilla Firefox и др. Хотя нет совершенно безопасного браузера, Internet Explorer представляет бóльший риск по части заражения из-за своей обширной пользовательской базы;
- использование файрволов и прокси-серверов для блокировки доступа к сайтам, известным как распространители spyware;
- использование hosts-файла, препятствующего возможности соединения компьютера с сайтами, известными как распространители spyware. Однако spyware легко могут обойти этот тип защиты, если производят соединение с удаленным хостом по IP-адресу, а не по имени домена;

- скачивание программ только из доверенных источников (предпочтительно с веб-сайтов производителя), поскольку некоторые spyware могут встраиваться в дистрибутивы программ;
- использование антивирусных программ с максимально «свежими» вирусными базами.

Adware

Определение.
Adware (синонимы AdvWare, Ad-Ware и т. п.) *— это приложение, предназначенное для загрузки на ПК пользователя информации рекламного характера для последующей демонстрации этой информации пользователю.*

Можно выделить **две категории Adware-программ**:

- **программы, распространяемые по Adware-лицензии.** Данные программы воспроизводят рекламу в качестве неявной оплаты за их использование, при этом реклама должна воспроизводиться только во время использования программы в контексте ее окон;
- **независимое приложение**, предназначенное для воспроизведения рекламы. Такие программы, как правило, маскируются от обнаружения и удаления пользователем и могут существенно досаждать пользователю. Рекламная информация обычно выводится в виде всплывающих окон, хотя известны и широко применяются другие методики демонстрации рекламы — например, внедрение рекламной информации в рабочий стол в виде обоев или с использованием возможностей размещения web-элементов на рабочем столе.

Можно сформулировать **ряд правил**, которых должна придерживаться корректная программа, распространяемая по Adware-лицензии.

Правило 1. При инсталляции на ПК программа должна предупредить пользователя о том, что является Adware приложением с разъяснением того, что конкретно понимается под термином «Adware». При этом инсталлятор должен предусматривать возможность отказа от установки приложения (а еще лучше — предлагать варианты установки — бесплатный Adware вариант или платный ShareWare вариант). Типовым примером «правильной» инсталляции является менеджер закачек FlashGet, который честно предлагает два варианта установки — Adware или ShareWare (FlashGet приведен в качестве примера

не случайно — ряд анти-SpyWare программ по неизвестной причине считают его шпионским ПО и удаляют).

Правило 2. Adware модуль должен быть или библиотекой, загружаемой Adware программой во время работы, или неразрывной частью Adware-программы. При этом загрузка Adware-модуля должна естественно происходить при запуске приложения, выгрузка и прекращение работы — при выгрузке приложения из памяти. Недопустимо внедрение Adware-модулей в другие приложения или их установка на автозапуск.

Правило 3. Adware-модуль должен воспроизводить рекламную информацию только в контексте вызывавшего его приложения. Недопустимо создание дополнительных окон, запуск сторонних приложений, открытие неких web-страниц.

Правило 4. Adware-модуль не должен выполнять действий, присущих программам категории SpyWare.

Правило 5. Adware-модуль должен деинсталлироваться вместе с установившим его приложением.

Это интересно знать.
К Adware-приложению в данной классификации предъявляются серьезные требования, и практически ни один Adware-модуль не удовлетворяет всем перечисленным требованиям.

На компьютеры пользователей **Adware** может попасть **двумя способами**:

- путем встраивания рекламных компонентов в бесплатное и условно-бесплатное программное обеспечение (freeware, shareware);
- путем несанкционированной установки рекламных компонентов при посещении пользователем «зараженных» веб-страниц.

Это интересно знать.
Большинство программ freeware и shareware прекращает показ рекламы после их покупки и/или регистрации. Подобные программы часто используют встроенные Adware-утилиты сторонних производителей.

В некоторых случаях эти Adware-утилиты остаются установленными на компьютере пользователя, и после регистрации программ, с которыми они изначально попали в операционную систему. При этом удаление Adware-компонента, используемого какой-либо программой

для показа рекламы, может привести к сбоям в функционировании этой программы.

Базовое назначение **Adware** данного типа — неявная форма оплаты программного обеспечения, осуществляемая за счет показа пользователю рекламной информации (рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство — разработчику **Adware**).

Adware помогает сократить расходы как разработчикам программного обеспечения (доход от **Adware** стимулирует их к написанию новых и совершенствованию существующих программ), так и самим пользователям.

В случае установки рекламных компонентов при посещении пользователем «зараженных» веб-страниц в большинстве случаев используются хакерские технологии: проникновение в компьютер через дыры в системе безопасности интернет-браузера, а также использование троянских программ, предназначенных для скрытой установки программного обеспечения (Trojan-Downloader или Trojan-Dropper). Adware-программы, действующие подобным образом, часто называют «Browser Hijackers».

Adware может выполнять нежелательные действия на вашем компьютере. Программа может следить за тем, какие сайты вы посещаете, адресовать вам всплывающие окна с рекламой на основе обычных результатов вашего поиска.

Некоторые **Adware** являются испытательными версиями программ. Отличие между этими двумя видами состоит в том, что **Adware**, как правило, содержат в себе рекламные компоненты, в то время как испытательные версии программ предлагают вам купить лицензированную копию данной программы.

Проблема с **Adware** состоит в том, что данная программа часто оказывается **Spyware** (программой-шпионом).

Очень тяжело указать разницу между **Adware**, испытательными версиями программ и вредоносными программами, так как функции всех трех частично совпадают.

Когда вы устанавливаете **Adware** на свой компьютер и выражаете согласие на пользование данной программой, **Adware** может стать программой-шпионом, если другой пользователь связывается с вашим компьютером. Таким образом, во время контакта с друзьями, за их компьютером начинает вестись наблюдение, также как и за вашим, без их на то согласия.

Adware в отличие от программ-шпионов не занимаются незаметным сбором и пересылкой личной информации, если пользователь не согласен с этим.

Это интересно знать.
Некоторые производители данных программ утверждают, что не имеют никакого сходства с программами-шпионами. Все действия, выполняемые программой, производятся только с согласия пользователя.

Сегодня в Интернете существует множество программ **Adware**. Также есть много доступных программ, помогающих пользователю найти, устранить или блокировать их. Чтобы продолжать оставаться свободными от этих программ, необходима хорошая программа, которая обнаруживает, помещает на карантин и удаляет **Adware** и программы-шпионы с компьютера. Эти программы создаются специально для обнаружения программ-шпионов и не работают с вирусами.

Tracking cookies

Tracking cookies (отслеживающие технологии) — файлы с малым количеством данных, таких как пароли и установочные параметры. Они могут быть полезными для вас, особенно если вы посещаете одни и те же сайты. Но с другой стороны Tracking cookies используются для отслеживания вашей работы в сети Интернет без вашего согласия и обеспечивают третьих лиц вашей личной информацией.

TrojanDownloader

Определение.
TrojanDownloader *— программы для несанкционированной загрузки и установки программного обеспечения.*

Программы из категории **Trojan-Downloader** (понятие **Trojan-Downloader** введено лабораторией Касперского) неоднократно упоминались, поэтому следует дать определение для данной категории программ.

Trojan-Downloader — это программа (модуль, ActiveX, библиотека ...), основным назначением которой является скрытная несанкцио-

нированная загрузка программного обеспечения из сети Интернет. Наиболее известным источником **Trojan-Downloader** являются хакерские сайты.

Сам по себе **Trojan-Downloader** как правило не несет прямой угрозы для компьютера — он опасен именно тем, что производит неконтролируемую загрузку программного обеспечения.

Trojan-Downloader применяются в основном для загрузки вирусов, троянских и шпионских программ. Наиболее известными являются **Trojan-Downloader**.IstBar, **Trojan-Downloader**.Win32.Dyfuca, **Trojan-Downloader**.Win32.Agent и ряд других. **Trojan-Downloader**.Win32.IstBar и **Trojan-Downloader**.Win32.Agent поставили своеобразный рекорд по количеству различных модификаций и своей вредоносности — их появление на компьютере приводит к резкому росту трафика и появлению на ПК множества посторонних программ.

Все программы категории TrojanDownloader можно условно подразделить на две категории:

- **универсальные Trojan-Downloader** — могут загружать любой программный код с любого сервера. Настройки могут храниться локально (в отдельном файле, реестре) или загружаться с определенного сайта;
- **специализированные** — предназначены для загрузки строго определенных типов троянских или шпионских программ. Адреса и имена файлов в таком случае жестко фиксированы и хранятся в теле программы.

Dialer

Программы категории **Dialer** (он-же часто называется «**порнозвонилка**» от названия Porn-**Dialer**, присвоенного им в классификации лаборатории Касперского) достаточно широко распространены и предназначены для решения ряда задач, связанных с дозвоном до заданного сервера и установления с ним модемной связи.

Применяются данные программы в основном создателями порносайтов, но страдают от них все — многие программы категории **Dialer** используют весьма изощренные способы установки (с использованием ActiveX, **Trojan-Downloader**), причем установка может быть инициирована при посещении практически любого сайта.

Организацию модемного соединения с сервером владельца **Dialer** может производить несколькими способами:

- **Dialer** может производить набор номера и установление соединения своими средствами;
- **Dialer** может создать новое соединение удаленного доступа;
- **Dialer** может изменить существующие соединения удаленного доступа.

В первых двух случаях **Dialer**, как правило, всячески привлекает внимание пользователя к себе и созданным им соединениям — копирует себя во все доступные места (в папку Program Files, Windows, Windows\System, папку «Пуск» и т. п.), создает ярлыки, регистрирует себя в автозапуске.

Часто кроме решения основной задачи программы типа **Dialer** выполняют задачи, свойственные программам других категорий (Adware, SpyWare, Trojan-Downloader). Некоторые **Dialer** устанавливают себя на автозапуск, внедряются в другие приложения.

Некоторые программы типа **Dialer** можно смело относить к троянским программам (а многие производители антивирусов считают **Dialer** троянской программой — на сайте производителей Norton Antivirus про **Dialer** говорится «троянская программа, предназначенная для ...»), в классификации лаборатории Касперского есть специальная категория **Trojan.Dialer**.

Кроме утилит дозвона к категории **Dialer** часто относят специализированные утилиты для просмотра порносайтов. Ведут они себя аналогично **Dialer**, только вместо модемного соединения соединяются с закрытими сайтами по Интернет.

BHO — Browser Helper Object

BHO (альтернативные названия — Browser Helper Object, Browser Plugin, Browser Bar, IE Bar, OE Bar и т. п., в классификации лаборатории Касперского есть категория подкатегория Toolbar, например AdWare. Toolbar.Azesearch) — это расширение браузера или программы электронной почты, как правило выполненное в виде дополнительной панели управления.

У **BHO** есть ряд достаточно опасных особенностей:

- **BHO** не являются процессами системы — они работают в контексте браузера и не могут быть обнаружены в диспетчере задач;
- **BHO** запускаются вместе с браузером и могут контролировать события, связанные с работой пользователя в Интернет (по сути, **BHO** для этого и предназначены);

- **BHO** обмениваются с сетью, используя API интеграции с браузером. Поэтому, с точки зрения большинства персональных FireWall обмен с Интернет ведет браузер. Как следствие, обнаружить такой обмен и воспрепятствовать ему очень сложно.

Ситуация отягощается тем, что многие **BHO**, входящие в категорию «SpyWare», передают информацию после запроса пользователя — это делает практически невозможным обнаружение постороннего обмена с Интернет, т. к. он идет на фоне полезного трафика.

Ошибки в работе **BHO** могут дестабилизировать работу браузера и приводить к трудно диагностируемым сбоям в его работе.

Hijacker

Буквальный перевод этого термина звучит как «налетчик», «грабитель», «воздушный пират». Это программа, которая выполняет на компьютере пользователя нежелательные для него действия, преследуя цели своих разработчиков. Производитель многих антивирусных средств относят программы категории **Hijacker** к троянским программам.

Задачей программ класса **Hijacker** является перенастройка параметров браузера, электронной почты или других приложений без разрешения и ведома пользователя.

Наиболее часто **Hijacker** применяется для изменения:

- стартовой страницы браузера — стартовая страница заменяется на адреса сайта создателей **Hijacker**;
- настройки системы поиска браузера (эти настройки хранятся в реестре). В результате при нажатии кнопки «Поиск» открывается адрес, установленный программой **Hijacker**;
- префиксов протоколов;
- уровней и настроек безопасности браузера;
- реакции браузера на ошибки;
- модификации списка адресов («Избранное») браузера.

Это интересно знать.

*В чистом виде **Hijacker** встречается сравнительно редко, т. к. чаще всего по выполняемым действиям программа может быть кроме категории «**Hijacker**» отнесена к категориям «Trojan»,»Dialer» или AdWare/SpyWare.*

Trojan — троянская программа

Определение.
Троянская программа *— это программа, которая выполняет действия, направленные против пользователя. Она собирает и передает владельцам конфиденциальную информацию о пользователе (эту категорию еще называют Trojan-Spy), выполняет несанкционированные или деструктивные действия.*

Из определения легко заметить, что троянская программа является «родственником» программ из категории SpyWare. Разница, как правило, в том, что SpyWare не имеют выраженного деструктивного действия и не передают конфиденциальную информацию о пользователе. Однако вопрос об отнесении программы к той или иной категории достаточно спорный (часто получается, что одна антивирусная компания считает некий модуль Adware, другая — троянской программой, третья — вообще игнорирует).

Backdoor — утилита скрытного удаленного управления и администрирования

Определение.
Backdoor *— это программа, основным назначением которой является скрытное управление компьютером.*

Backdoor можно условно подразделить на две категории.

Категория 1. **Backdoor**, построенные по технологии Client-Server. Такой **Backdoor** состоит как минимум из двух программ — небольшой программы, скрытно устанавливаемой на поражаемый компьютер, и программы управления, устанавливаемой на компьютер злоумышленника. Иногда в комплекте идет еще и программа настройки.

Категория 2. **Backdoor**, использующие для удаленного управления встроенный telnet, web или IRC сервер. Для управления таким **Backdoor** не требуется специальное клиентское программное обеспечение. К примеру, известны **Backdoor**, которые подключался к заданному IRC серверу и используют его для обмена со злоумышленником.

Основное назначение Backdoor — скрытное управление компьютером. Как правило, **Backdoor** позволяет копировать файлы с пораженного компьютера, и наоборот, передавать на пораженный компьютер

файлы и программы. Кроме того, обычно **Backdoor** позволяет получить удаленный доступ к реестру, производить системные операции (перезагрузку ПК, создание новых сетевых ресурсов, модификацию паролей и т. п.).

Будьте осторожны.
Backdoor *по сути открывает атакующему «черный ход» на компьютер пользователя. Опасность* ***Backdoor*** *увеличилась в последнее время в связи с тем, что многие современные сетевые и почтовые черви или содержат в себе* ***Backdoor****-компоненту, или устанавливают ее после заражения ПК.*

RootKit

Термин **RootKit** исторически пришел из мира Unix, где под этим термином понимается набор утилит, которые хакер устанавливает на взломанном им компьютере после получения первоначального доступа. Это, как правило, хакерский инструментарий (снифферы, сканеры) и троянские программы, замещающие основные утилиты Unix. **RootKit** позволяет хакеру закрепиться во взломанной системе и скрыть следы своей деятельности.

В системе Windows под **RootKit** принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО.

Кроме того, многие **RootKit** могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие **RootKit** устанавливают в систему свои драйверы и сервисы (они, естественно, также являются «невидимыми»).

В последнее время угроза **RootKit** становится все более актуальной, т. к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать **RootKit**-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи **RootKit**-технологии.

1.2. Клавиатурные «шпионы»

Понятие клавиатурных «шпионов»

Клавиатурные шпионы образуют категорию вредоносных программ, представляющую большую угрозу для безопасности пользователя. Они не являются вирусами, т. к. не обладают способностью к размножению.

Определение.
Клавиатурные шпионы *— это программа для скрытной записи информации о нажимаемых пользователем клавишах.*

У термина «клавиатурный шпион» есть ряд синонимов: Keyboard Logger, KeyLogger; реже встречается термины «snoop», «snooper» (от англ. *snoop* — буквально «человек, вечно сующий нос в чужие дела»).

Как правило, современные клавиатурные шпионы не просто записывает коды вводимых клавиш. Они «привязывают» клавиатурный ввод к текущему окну и элементу ввода.

Кроме того, многие клавиатурные шпионы:

- отслеживают список запущенных приложений;
- умеют делать «снимки» экрана по заданному расписанию или событию;
- шпионить за содержимым буфера обмена;
- решать ряд задач, нацеленных на скрытное слежение за пользователем.

Записываемая информация сохраняется на диске, и большинство современных клавиатурных шпионов могут формировать различные отчеты, могут передавать их по электронной почте или http/ftp-протоколу. Кроме того, ряд современных клавиатурных шпионов пользуются **RootKit**-технологиями для маскировки следов своего присутствия в системе.

Для системы клавиатурный шпион, как правило, безопасен. Однако он чрезвычайно опасен для пользователя. С его помощью можно перехватить пароли и прочую конфиденциальную информацию, вводимую пользователем. К сожалению, известны сотни разнообразных кейлоггеров. Причем многие из них не определяются антивирусами.

Принцип действия

При возникновении неких событии ввода (нажатии клавиш, перемещении мыши) события обрабатываются соответствующим драйвером и помещается в системную очередь аппаратного ввода. В системе имеется особый поток необработанного ввода, называемый RIT (Raw Input Thread), который извлекает события из системной очереди и преобразует их в сообщения.

Полученные сообщения помещаются в конец очереди виртуального ввода одного из потоков (виртуальная очередь потока называется VIQ — Virtualized Input Queue). При этом RIT сам выясняет, в очередь какого конкретно потока необходимо поместить событие. Для событий мыши поток определяется поиском окна, над которым расположен курсор мыши.

Клавиатурные события отправляются только одному потоку — так называемому **активному потоку** (т. е. потоку, которому принадлежит окно, с которым работает пользователь). На самом деле это не совсем так — в частности, на рисунке показан поток A, не имеющий очереди виртуального ввода.

В данном случае получатся, что потоки A и B совместно используют одну очередь виртуального ввода. Это достигается при помощи вызова API функции AttachThreadInput, которая позволяет одному потоку подключиться к очереди виртуального ввода другого потока.

Следует отметить, что поток необработанного ввода отвечает за обработку специальных сочетаний клавиш, в частности Alt+Tab и Ctrl+Alt+Del.

Слежение за клавиатурным вводом при помощи ловушек

Данная методика является классической для клавиатурных шпионов. **Суть метода** состоит в применении механизма ловушек (hook) операционной системы. Ловушки позволяют наблюдать за сообщениями, которые обрабатываются окнами других программ.

Установка и удаление ловушек производится при помощи хорошо документированных функций API библиотеки user32.dll (функция SetWindowsHookEx позволяет установить ловушку, UnhookWindowsHookEx — снять ее). При установке ловушки указывается тип сообщений, для которых должен вызываться обработчик ловушки.

В частности, есть **два специальных типа ловушки** WH_KEYBOARD и WH_MOUSE — для регистрации событий клавиатуры и мыши соответственно. Ловушка может быть установлена для заданного потока и для всех потоков системы. Ловушка для всех потоков системы очень удобна для построения клавиатурного шпиона.

Код обработчика событий ловушки должен быть расположен в DLL. Это требование связано с тем, что DLL с обработчиком ловушки проецируется системой в адресное пространство всех GUI процессов. Интересной особенностью является то, что проецирование DLL происходит не в момент установки ловушки, а при получении GUI процессом первого сообщения, удовлетворяющего параметрам ловушки.

Методика ловушек достаточно проста и эффективна, но у нее есть ряд **недостатков**. Первым недостатком можно считать то, что DLL с ловушкой проецируется в адресное пространство всех GUI процессов, что может применяться для обнаружения клавиатурного шпиона. Кроме того, регистрация событий клавиатуры возможна только для GUI приложений, это легко проверить при помощи демонстрационной программы.

Слежение за клавиатурным вводом при помощи опроса клавиатуры

Данная методика основана на периодическом опросе состояния клавиатуры. Для опроса состояния клавиш в системе предусмотрена специальная функция GetKeyboardState, возвращающая массив из 255 байт, в котором каждый байт содержит состояние определенной клавиши на клавиатуре. Данный метод уже не требует внедрения DLL в GUI процессы и в результате шпион менее заметен.

Однако изменение статуса клавиш происходит в момент считывания потоком клавиатурных сообщений из его очереди, и в результате подобная методика работает только для слежения за GUI приложениями. От этого недостатка свободна функция GetAsyncKeyState, возвращающая состояние клавиши на момент вызова функции.

Недостатком клавиатурных шпионов такого типа является необходимость периодического опроса состояния клавиатуры с достаточно высокой скоростью, не менее 10—20 опросов в секунду.

Клавиатурный шпион на базе драйвера

Данный метод более эффективен, чем описанные выше методы. Возможны как минимум два варианта реализации этого метода — написание и установка в систему своего драйвера клавиатуры вместо штатного или установка драйвера-фильтра.

Аппаратные клавиатурные шпионы

В ходе решения задач по защите от утечки информации часто рассматривают только различные программные средства для шпионажа за работой пользователя. Однако, кроме программных, возможны и **аппаратные средства**:

- установка устройства слежения в разрыв кабеля клавиатуры (например, устройство может быть выполнено в виде переходника PS/2);
- встраивание устройства слежения в клавиатуру;
- считывание данных путем регистрации ПЭМИН (побочных электромагнитных излучений и наводок);
- визуальное наблюдение за клавиатурой.

Аппаратные клавиатурные шпионы встречаются намного реже, чем программные. Однако при проверке особо ответственных компьютеров (например, применяемых для совершения банковских операций) о возможности аппаратного слежения за клавиатурным вводом не следует забывать.

Методики поиска клавиатурных шпионов

Поиск по сигнатурам. Данный метод не отличается от типовых методик поиска вирусов. Сигнатурный поиск позволяет однозначно идентифицировать клавиатурные шпионы, при правильном выборе сигнатур вероятность ошибки практически равна нулю. Однако сигнатурный сканер сможет обнаруживать заранее известные и описанные в его базе данных объекты.

Эвристически алгоритмы. Как очевидно из названия, это методики поиска клавиатурного шпиона по его характерным особенностям. Эвристический поиск носит вероятностный характер. Как показала практика, этот метод наиболее эффективен для поиска клавиатурных шпионов самого распространенного типа — основанных на ловушках.

Однако подобные методики дают много ложных срабатываний. Мои исследования показали, что существуют сотни безопасных программ, не являющихся клавиатурными шпионами, но устанавливающих ловушки для слежения за клавиатурным вводом и мышью. Наиболее распространенный примеры — программы Punto Switcher, словарь Lingvo, программное обеспечение от мультимедийных клавиатур и мышей.

Мониторинг API функций, используемых клавиатурными шпионами. Данная методика основана на перехвате ряда функций, применяемых клавиатурным шпионом — в частности, функций SetWindowsHookEx, UnhookWindowsHookEx, GetAsyncKeyState, GetKeyboardState. Вызов данных функций каким-либо приложением позволяет вовремя поднять тревогу, однако проблемы многочисленных ложных срабатываний будут аналогичны предыдущему методу.

Отслеживание используемых системой драйверов, процессов и сервисов. Это универсальная методика, применимая не только против клавиатурных шпионов. В простейшем случае можно применять программы типа Kaspersky Inspector или Adinf, которые отслеживают появление в системе новых файлов.

Программы для поиска и удаления клавиатурных шпионов

Любой антивирусный продукт. Все антивирусы в той или иной мере могут находить клавиатурные шпионы, однако клавиатурный шпион не является вирусом и в результате пользы от антивируса мало.

Утилиты, реализующие механизм сигнатурного поиска и эвристические механизмы поиска. Примером может служить утилита AVZ, сочетающая сигнатурный сканер и систему обнаружения клавиатурных шпионов на базе ловушек.

Специализированные утилиты и программы, предназначенные для обнаружения клавиатурных шпионов и блокирования их работы. Подобные программы наиболее эффективны для обнаружения и блокирования клавиатурных шпионов, поскольку, как правило, могут блокировать практически все разновидности клавиатурных шпионов.

Из специализированных программ интерес могут представлять коммерческие продукты PrivacyKeyboard и Anti-keylogger (http://www.bezpeka.biz/).

Программа Anti-keylogger работает в фоновом режиме и производит обнаружение программ, подозреваемых в слежении за клавиатурой. В

случае необходимости можно вручную разблокировать работу любой из обнаруженных. Для обнаружения клавиатурных шпионов не применяются базы сигнатур, обнаружение ведется эвристическими методами. Тестирование программы показало, что она эффективно противодействует клавиатурным шпионам, основанным на применении ловушек, циклического опроса и клавиатурного драйвера-фильтра.

Другим примером может служить программа **Advanced Anti Keylogger** (http://www.anti-keylogger.net). В режиме обучения данная программа по логике работы напоминает Firewall — при обнаружении подозрительной активности выводится предупреждение с указанием имени и описания программы. Пользователь может выбрать действие на сеанс (разрешить, запретить), или создать постоянное правило для правило для приложения. В ходе тестов Advanced Anti Keylogger уверенно обнаружил все основные разновидности клавиатурных шпионов (на базе ловушки, циклического опроса, драйвера-фильтра). Настройки программы защищаются паролем, который задается в ходе инсталляции.

1.3. Методики обнаружения вредоносного программного обеспечения

Пути решения проблемы при заражении компьютера

Практика показывает, что разработчики антивирусных и анти-SpyWare программных продуктов не успевают оперативно вносить в базы сигнатуры всех разновидностей вредоносных программ. В результате независимо от применяемого антивирусного пакета любой пользователь может рано или поздно столкнуться с тем, что на его компьютер попадет вредоносная программа, которую не сможет обнаружить и удалить применяемый пользователем антивирус.

Хуже всего дело обстоит с **AdWare и SpyWare программами** — далеко не все производители антивирусов включают такие программы в свои базы. Кроме того, ожидать добавления вредоносной программы в базы антивируса можно достаточно долго, поскольку для этого разработчики антивируса должны получить ее образец.

В результате для пользователя получается замкнутый круг, выйти из которого можно тремя путями:

- переустановить систему;
- пригласить специалистов для консультации;
- попробовать самостоятельно обнаружить вредоносную программу и отправить ее разработчикам антивирусных пакетов.

Опишу набор бесплатных утилит, которые могут быть полезны для поиска и уничтожения большинства вредоносных программ, а также основные методики проверки компьютера.

Утилиты для анализа ПК

Утилита FileMon (производитель SysInternals). Утилита позволяет осуществлять мониторинг всех файловых операций в реальном времени, распространяется бесплатно. Кроме файловых операций FileMon позволяет осуществлять мониторинг операций с именованными каналами (Named Pipes), Mail Slot и сетевыми ресурсами.

FileMon не нуждается в инсталляции и может быть запущен с компакт-диска или из сетевой папки. Необходимо учесть, что внутри исполняемого файла filemon.exe хранятся драйвера, которые извлекаются и инсталлируются в момент запуска.

Полезной особенностью программы является возможность настраиваемой фильтрации регистрируемых событий.

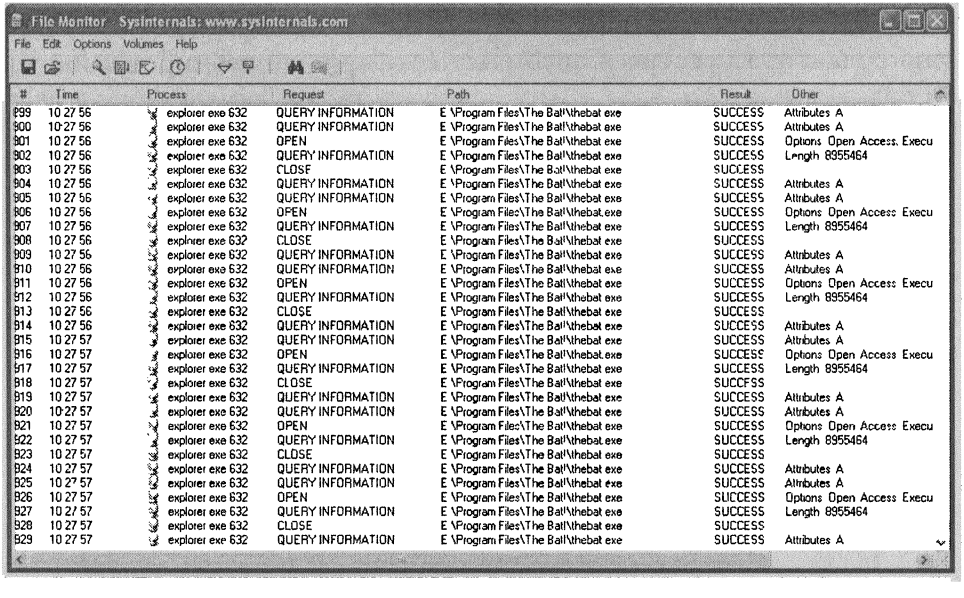


Рис. 2.1. Утилита FileMon

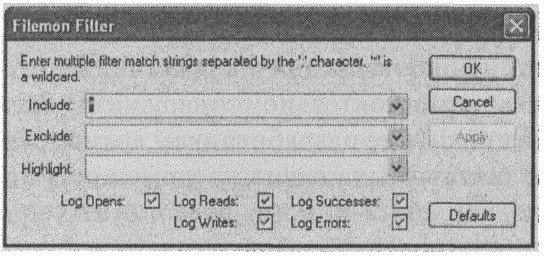


Рис. 2.2. Настройка фильтрации в утилите FileMon

Кроме фильтра предусмотрен пункт меню «Volumes», который позволяет включить или выключить мониторинг для каждого тома.

Протокол утилиты может быть сохранен в текстовый файл для последующего анализа. Разделителем полей протокола является символ табуляции, что позволяет импортировать его в Microsoft Excel.

Утилита RegMon (производитель SysInternals). Утилита позволяет осуществлять мониторинг всех операций с реестром в реальном времени, распространяется бесплатно. Интерфейс данной утилиты аналогичен FileMon.

Исполняемый файл использует для работы драйвер, который хранится внутри исполняемого файла и устанавливаются в момент запуска программы. Запись событий можно временно приостановить при помощи пункта меню «File\Capture events».

Двойной щелчок мышью на строке протокола приводит к открытию редактора реестра и автоматическому позиционированию на

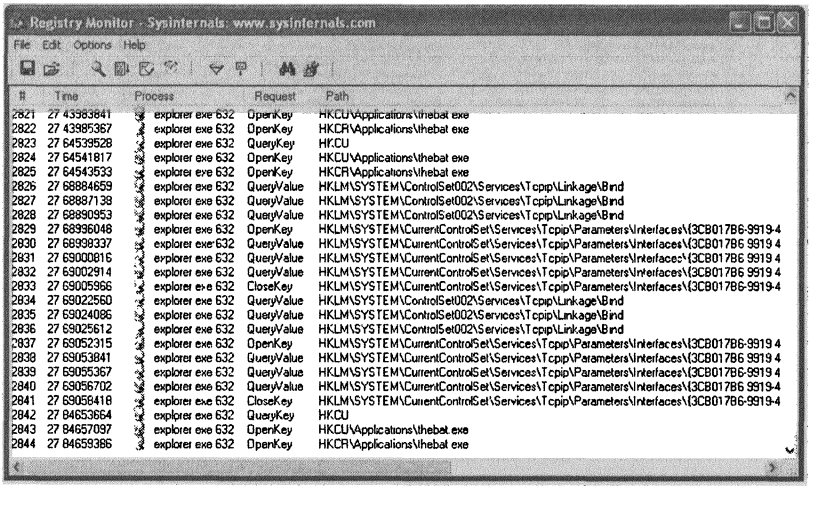


Рис. 2.3. Утилита RegMon

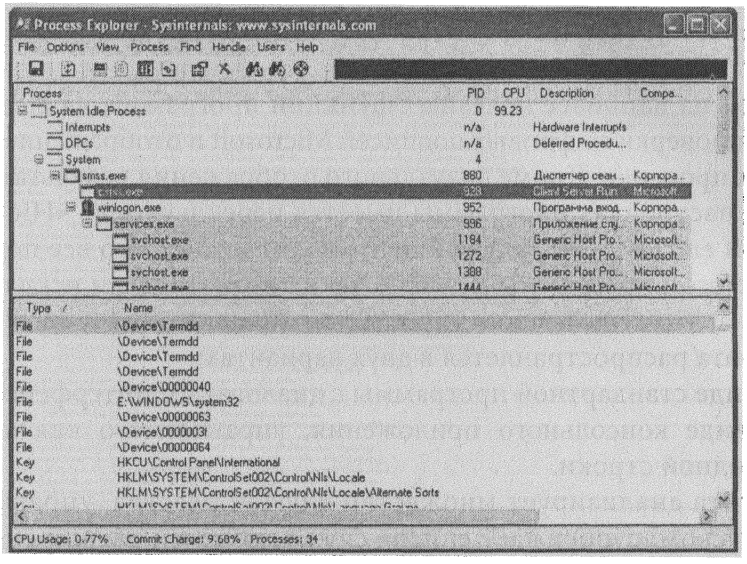


Рис. 2.4. *Process Explorer*

соответствующий ключ реестра. Как и в случае с FileMon протоколы утилиты могут быть сохранены в текстовый файл для анализа.

Process Explorer (производитель SysInternals). Основной задачей Process Explorer является просмотр списка запущенных процессов. Для каждого процесса отображаются потоки, используемые им библиотеки, Handle (с расшифровкой типа Handle и отображением уточняющей информации). Помимо просмотра списка процессов программа может выполнять ряд полезных сервисных функций, в частности осуществлять поиск процесса по его окну и составлять список процессов, использующих указанную библиотеку.

Для каждого процесса есть возможность просмотра детализированной информации. Детализированная информация включает данные о потоках, прослушиваемых портах TCP/UDP, параметры безопасности, переменные окружения, список найденных в исполняемом файле (на диске и в памяти процесса) текстовых данных с возможностью поиска и сохранения найденной информации для анализа.

Еще одной заслуживающей внимания возможностью утилиты является встроенная поддержка механизма проверки цифровых подписей файлов.

Утилита Autoruns (производитель SysInternals). Утилита является диспетчером автозапуска с расширенными возможностями. Утилита

анализирует практически все способы автозапуска, применяемые вредоносными программами.

Одной из наиболее полезных функций программы является поддержка проверки цифровых подписей Microsoft и отображение результатов их проверки. Кроме визуального отображения результатов проверки в настройках программы имеется переключатель «Hide signed Microsoft entries». Его включение приводит к тому, что все подписанные Microsoft программы и библиотеки автоматически исключаются из списка, что существенно упрощает его анализ.

Утилита распространяется в двух вариантах:

- в виде стандартной программы с диалоговым интерфейсом;
- в виде консольного приложения, управляемого ключами командной строки.

Утилита анализирует множество ключей реестра, управляющих автозапуском, отображает список служб, модулей расширения проводника, BHO (Browser Helper Object) и панели Internet Explorer, назначенные задания. Любая библиотека или программа может быть временно удалена из автозагрузки, что позволяет на время отключить запуск подозрительных программ и библиотек.

Утилита Sigcheck (производитель SysInternals). Эта небольшая консольная утилита позволяет просматривать и проверять цифровые подписи указанного файла. Утилита очень полезна для идентификации системных файлов, которые имеют цифровую подпись Microsoft.

Утилита поддерживает ряд ключей, однако в простейшем случае достаточно передать ей единственный параметр — полное имя проверяемого файла. В результате проверки отображается информация о найденных цифровых подписях и результатах их проверки. Следует отметить, что поле «Publisher» в протоколе программы необходимо читать очень внимательно — известны программы, снабженные корректной цифровой подписью от «Micrsoft», «Mikrosoft», «Mirosoft» — т. е. название компании специально выбрано очень похожее на «Microsoft» в расчете на то, что пользователь не обратит внимания на небольшие различия в написании.

Утилита HijackThis (http://www.tomcoyote.org/hjt/). Протоколы утилиты HijackThis являются стандартом для многих конференций, посвященных информационной безопасности. Утилита анализирует системные настройки и отображает их на экране в виде списка. Важно отметить, что утилита не анализирует собранную информацию — предполагается, что пользователь самостоятельно примет решение о

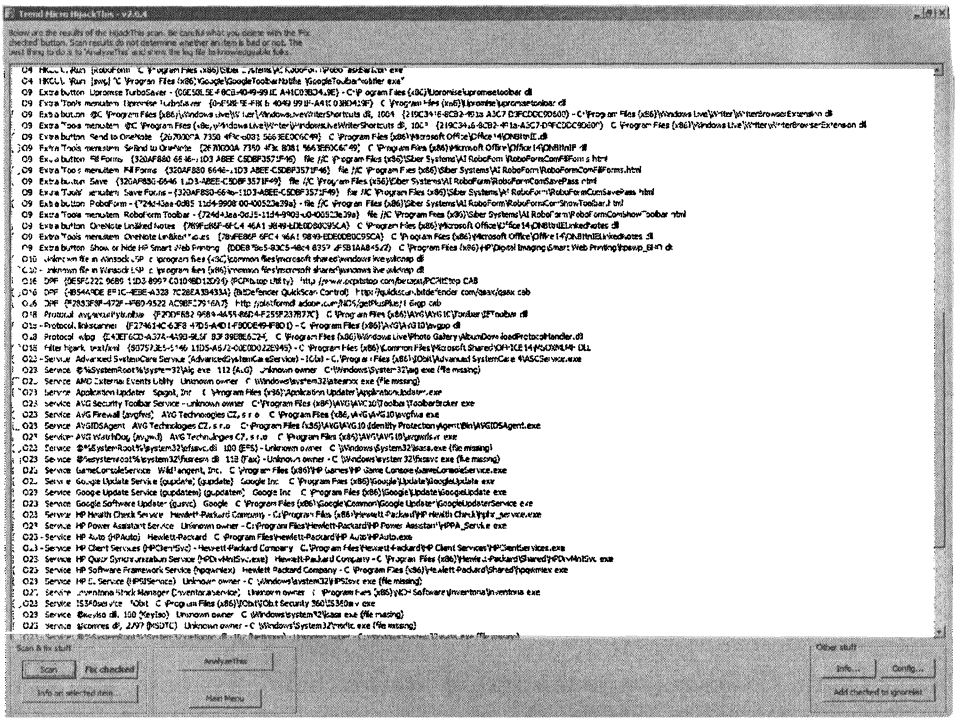


***Рис. 2.5.** Утилита HijackThis*

том, какие элементы появились в результате деятельности вредоносных программ.

Пользователь может отметить один или несколько элементов, после нажатия кнопки «Fix» утилита производит их исправление или удаление. Утилита позволяет сохранять текстовые протоколы с результатами анализа, протокол достаточно легко анализировать вручную или с помощью автоматизированных анализаторов.

Утилита a-squared HiJackFree (http://www.hijackfree.com/en/).

Данная программа представляет собой универсальный анализатор, отображающий элементы автозапуска (включая многие экзотические), модули расширения Explorer, службы и запущенные процессы, открытые порты, содержимое файла Hosts. По результатам анализа формируется XML протокол, который может быть сохранен или передан для анализа на сайт http://www.hijackfree.com. Результаты анализа отображаются немедленно, полученный в результате анализа HTML протокол можно сохранить. Однако следует помнить, что для формирования протокола результаты анализа вашего компьютера передаются компании a-squared.

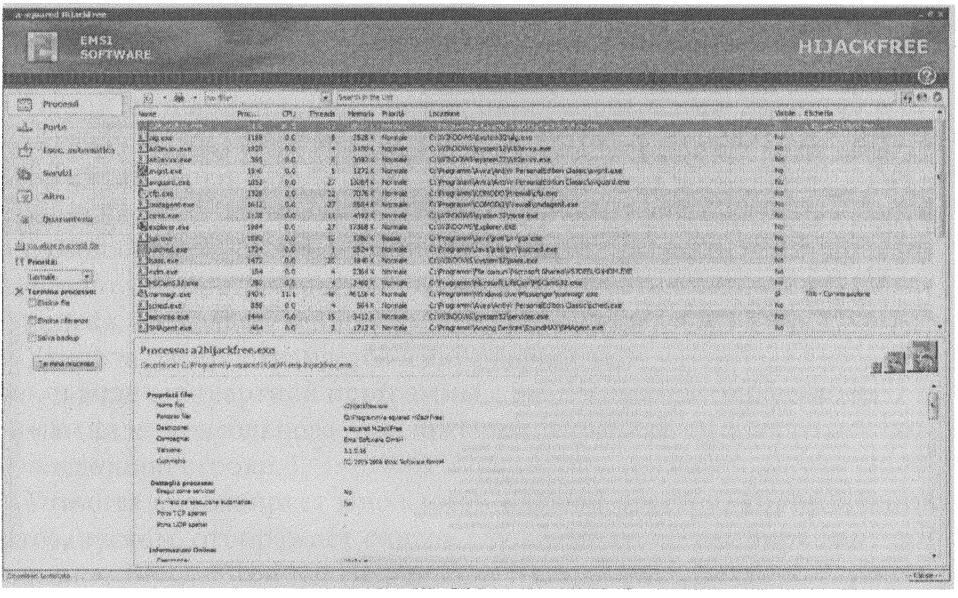


Рис. 2.6. *Утилита a-squared HiJackFree*

Утилита TDIMon (производитель SysInternals). Утилита TDIMon предназначена для мониторинга сетевой активности приложений. В протоколе утилиты регистрируются обмен приложений по протоколам TCP и UDP. Программа не нуждается в инсталляции и может оказаться весьма полезной для обнаружения программ, ведущих скрытный обмен с сетью.

Утилита AVZ (http://z-oleg.com/secur/). Утилита является прямым аналогом программ Trojan Hunter и LavaSoft Ad-aware 6. Первичной задачей программы является удаление AdWare, SpyWare и троянских программ. Особенностью программы AVZ является возможность настройки реакции программы на каждую из категорий вредоносных программы. Например, можно задать режим уничтожения найденных вирусов и троянских программ, но заблокировать удаление AdWare.

Другой особенностью AVZ являются многочисленные эвристические проверки системы, не основанные на механизме поиска по сигнатурам: это поиск RootKit, клавиатурных шпионов, различных Backdoor по базе типовых портов TCP/UDP. Подобные методы поиска позволяют находить новые разновидности вредоносных программ.

Начиная с версии 4.29, в AVZ локализация интерфейса и протоколов выполняется на основе обновляемых баз, на текущий момент поддерживается русский и английский язык, выбор языка произво-

дится автоматически или вручную при помощи параметра командной строки Lang или профиля локализации.

Выбор языка идет автоматически (на русскоязычной системе русский, на остальных — английский) или вручную через параметры командной строки и профиль локализации. Параметр командной строки — lang=X, где X — название локализации, RU для русского, EN — для английского. Т.е. для принудительного включения русского языка нужно вызывать AVZ в виде avz.exe lang=ru (соответственно для принудительного включения английского avz.exe lang=en)

Ограничения программы рассмотрю ниже.

Ограничение 1. Т. к. утилита направлена, в первую очередь, на борьбу с SpyWare и AdWare модулями, и в настоящий момент она не поддерживает проверку архивов некоторых типов, PE упаковщиков и документов. Для борьбы со SpyWare в этом просто нет надобности. Тем не менее, утилита совершенствуется и появление подобных функций планируется.

Ограничение 2. Утилита не лечит программы, зараженные компьютерными вирусами. Для качественного и корректного лечения зараженной программы необходимы специализированные антивирусы (например, антивирус Касперского, DrWeb, Norton Antivirus, Panda и т. п.). Делать нечто похожее на них (изобретая тем самым велосипед) у меня нет никакого желания, тем более что вирусы такого рода встречаются все реже.

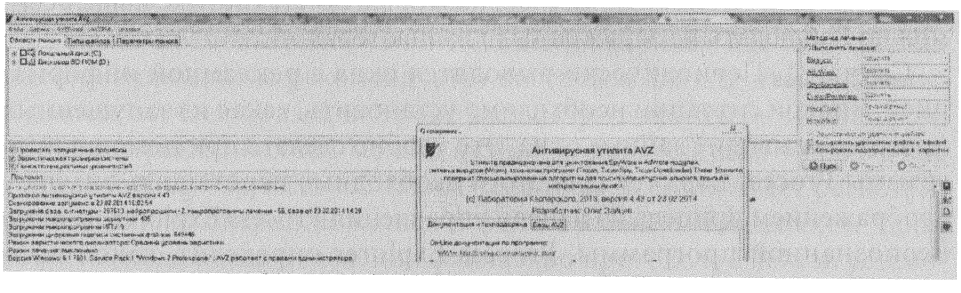


Рис. 2.7. Утилита AVZ

Полезные On-Line сервисы

http://www.hijackthis.de/en. Автоматический анализатор протоколов утилиты HijackThis. Работает только с протоколами последней версии данной утилиты, по результатам анализа генерирует протокол с указанием, на какие позиции следует обратить внимание.

http://www.virustotal.com/. Проверка файла несколькими антивирусами. В настоящий момент проверка переданного для анализа файла проводится при помощи 19-ти антивирусных пакетов.

http://virusscan.jotti.org/. Проверка файла несколькими антивирусами. На этом сайте проверка файла производится при помощи 13-ти антивирусов, и кроме проверки антивирусами проводится экспресс-анализ файла — вычисление его MD5 суммы, попытка определения упаковщика и оценка «степени опасности» файла по некоторым критериям создателей сайта.

http://virusinfo.info/. Русскоязычная конференция, полностью посвященная вирусологии, борьбе с AdWare/SpyWare программами и защите компьютера. Для начинающего пользователя ценность представляет раздел «Помогите», в котором рассматриваются проблемы пользователей, анализируются полученные от пользователей протоколы и подозрительные файлы.

http://forum.ixbt.com/. Русскоязычная конференция, содержит подразделы «Системное администрирование, безопасность», «Техподдержка» и «Программы: Интернет», в которых обсуждаются вопросы безопасности, антивирусные программы, Firewall и методы обнаружения вирусов.

Возможные проблемные ситуации

Рассмотрим несколько случаев, которые по статистике чаще всего можно наблюдать на зараженных компьютерах.

Случай 1. Периодически выводятся окна с рекламной информацией. В такой ситуации необходимо установить, какая из запущенных программ выводит данные окна. Это удобно сделать при помощи программы Process Explorer. Для этого необходимо перетащить значок с изображением прицела из панели управления Process Explorer на окно неопознанной программы. Process Explorer определит, какой программе принадлежит данное окно. Если обнаружится, что окно принадлежит Internet Explorer, то необходимо проанализировать загруженные им библиотеки и модули расширения (BHO). Кроме того, Process Explorer показывает процессы в виде древовидного списка — стоит обратить внимание на то, какой процесс является родительским для «подозреваемого».

Случай 2. Стартовая страница Internet Explorer периодически изменяется на некую страницу X. Настройки IE хранятся в реестре, поэтому

для обнаружения изменяющего страницу «вредителя» очень удобно применить утилиту RegMon. После запуска утилиты необходимо настроить фильтр утилиты RegMon, указав в качестве образца адрес X или его фрагмент. Затем остается только восстановить стартовую страницу и дождаться ее изменения — далее по протоколу RegMon можно установить, какой процесс выполнил данную операцию.

Случай 3. Изменяются настройки Internet Explorer, в том числе недоступные из диалога «свойства обозревателя». Чаще всего изменяется страница поиска или префиксы протоколов, замена стартовой страницы может рассматриваться как частный случай этой ситуации. Методика обнаружения ответственного за это вредоносного процесса аналогична случаю с подменой стартовой страницы, в настройке фильтра RegMon в поле Include рекомендуется задать образец «Microsoft\Internet Explorer» и оставить включенной опции «Log Writes» и «Log Successes». В результате будет фиксироваться все изменения настроек с указанием, какая программа производит изменение. Для восстановления настроек можно применить кнопку «Сброс параметров» на закладке «Свойства программы» в окне «Свойства обозревателя» или использовать восстановление системы в AVZ. В обоих случаях это приведет к сбросу все настроек на значения по умолчанию.

Случай 4. На рабочем столе (на диске, в определенных папках) периодически появляются посторонние файлы и ярлыки. Для определенности предположим, что на рабочем столе появляется файл **Dialer.exe**, причем через некоторое время после его удаления файл появляется снова. Воспользуемся утилитой FileMon, причем для уменьшения размеров протокола рекомендуется настроить фильтр этой утилиты. В нашем случае образец в строке Include фильтра будет «**Dialer.exe**», из всех переключателей можно оставить включенным только «Log Writes» и «Log Successes». С таким фильтром FileMon будет регистрировать только операции записи в файл с именем «**Dialer.exe**». Далее остается подождать появления файла и по протоколу FileMon установить создающее его приложение.

Случай 5. После удаления вредоносной программы (вручную или при помощи антивируса) возникли проблемы с доступом в Интернет. Подобная ситуация, как правило, возникает в случае удаления модуля, зарегистрированного в качестве расширения Winsock. Проанализировать зарегистрированные модули расширения Winsock можно в AVZ — меню Сервис, пункт «Менеджер Winsock SPI». Менеджер оснащен автоматическим анализатором, который в состо-

нии обнаружить типовые ошибки и исправить их. Список ошибок можно посмотреть на закладке «Поиск ошибок», там же имеется кнопка «Автоматическое исправление найденных ошибок». В большинстве случаев анализатор AVZ в состоянии справиться с ошибками. Если он не поможет (а такое возможно в случае серьезного повреждения настроек, например, полного удаления ключей реестра, хранящих настройку), рекомендуется обратьcя к статьям 299357, 817571 и 811259, размещенным на сайте Microsoft (http://support.microsoft.com/kb/<номер статьи>). В данных статьях подробно рассмотрены методики ручного сброса, восстановления и проверки настроек протоколов TCP/IP.

Случай 6. Изменились обои и настройки рабочего стола, меню настройки рабочего стола недоступно. Подобная ситуация все чаще регистрируется в последние месяцы и связана с оригинальной методикой демонстрации рекламы — вместо отображения рекламной информации в отдельных окнах современные троянские программы внедряют ее в рабочий стол. В ряде случаев можно восстановить настройки вручную, однако некоторые троянских программы блокирую вызов меню настройки при помощи параметров в ключе реестра Software\Microsoft\Windows\CurrentVersion\Policies. Для разблокировки меню и сброса настроек можно применить «Восстановление системы» AVZ. Там предусмотрена специальная функция «Восстановление настроек рабочего стола».

Случай 7. Нарушилось обновление антивирусных программ, хотя доступ в Интернет работает нормально. В такой ситуации рекомендуется проверить файл HOSTS, возможно, в нем появились дополнительные записи. Отследить модифицирующий файл hosts процесс достаточно легко при помощи утилиты FileMon. Восстановить файл проще всего вручную: в нем должна быть единственная строка вида «127.0.0.1 localhost». Для редактирования фала Hosts можно воспользоваться программами HiJackFree или HijackThis.

ШПИОНСКИЕ И АНТИШПИОНСКИЕ ПРОГРАММЫ СМАРТФОНОВ И МОБИЛЬНЫХ ТЕЛЕФОНОВ

Главной «шпионской штучкой» сегодня стали мобильные средства связи. Шпионские программы способны контролировать активность на мобильном устройстве, на которое установлены. Текстовые сообщения, набираемые на телефоне, входящие и исходящие вызовы вместе с продолжительностью звонка, SMS, MMS, электронная почта, любые данные, полученные или переданные через Интернет, координаты устройства — все это будет доступно для просмотра в любое время суток. Лучшие шпионские программы также прослушивают и записывают разговоры через мобильное устройство, превратив телефон в настоящий электронный жучок.

3.1. Шпионские программы для мобильных телефонов, смартфонов, коммуникаторов

Что такое «умные телефоны»

Смартфон (англ. *smartphone* — умный телефон) — мобильный телефон, сравнимый с карманным персональным компьютером. Часто используется и термин «**коммуникатор**», карманный персональный компьютер, дополненный функциональностью мобильного телефона. Термин же «коммуникатор» сейчас используется в основном как синоним для смартфона.

Смартфоны характеризуют продвинутые мультимедийные функции (качественная камера, расширенные возможности воспроизведения видео файлов, улучшенные музыкальные способности), наличие Wi-Fi, GPS.

В настоящее время граница между «обычными» мобильными телефонами и смартфонами все больше стирается. Современные мобилки (за исключением самых дешевых моделей) обладают функциональностью, некогда присущей только смартфонам, например, электронная почта и HTML-браузер, а также многозадачностью.

Современные телефоны (модели средней ценовой категории и выше) прекрасно справляются со многими задачами, выходящими за рамки телефонных:

- работа с электронной почтой;
- просмотр текстовых документов и электронных таблиц;
- работа с планировщиком задач.

Расширение функциональности телефонов возможно за счет J2ME-программ, которые поддерживаются практически всеми мобильными телефонами, смартфонами и коммуникаторами. Экран целого ряда мобильных телефонов не уступает большинству смартфонов, большинство моделей оснащены разъемом для **карты памяти**.

Это интересно знать.

Программы, написанные специально для операционной системы смартфона или коммуникатора, являются полноценными скомпилированными в двоичный код последовательностями низкоуровневых микропроцессорных команд.

С течением времени продукты, называемые смартфонами и коммуникаторами, сближались. Размеры коммуникаторов уменьшались, а телефонные функции выходили на первый план. Размеры смартфонов наоборот, увеличивались, а функциональность достигла уровня КПК.

Очередной этап развития смартфонов начался после успешного выхода на рынок мобильного телефона **iPhone** от фирмы Apple. Операционная система данного устройства, позиционируемого как смартфон, была функционально урезана из маркетинговых соображений. Так, была ограничена возможность установки программ сторонних производителей, имелись ограничения в части многозадачности. Тем не менее, благодаря удачному дизайну и грамотной политике продвижения, это устройство стало законодателем мод и установило новые стандарты для бесклавиатурных устройств.

Если в середине 2000-х годов размеры экрана большинства коммуникаторов и смартфонов составляли 2,4—2,8 дюйма с разрешением

320×240 точек, то в настоящее время типичным стал экран 3—5" с разрешением 480×320 (iPhone, Android), 800×480 (Android), 640×360 (S60v5, Symbian[3]), 960×640 (iPhone 4/4S, Android) 1280×720 (Android).

Операционные системы мобильных устройств и вредоносные программы

Операционная система обычных мобильных телефонов закрыта для сторонних разработчиков. А вот смартфоны и коммуникаторы отличаются от обычных мобильных телефонов наличием достаточно развитой операционной системы, открытой для разработки программного обеспечения сторонними разработчиками.

Установка дополнительных приложений позволяет значительно улучшить функциональность смартфонов и коммуникаторов по сравнению с обычными мобильными телефонами.

Наличие полнофункциональной операционной системы делает смартфоны и коммуникаторы более привлекательными в глазах большинства пользователей. Открытость операционной системы смартфонов и коммуникаторов порождает еще одну проблему, хорошо знакомую пользователям персональных компьютеров — компьютерные вирусы и другие **вредоносные программы**.

Для защиты от этой опасности большинством ведущих разработчиков антивирусного ПО созданы специальные версии антивирусных программ для мобильных операционных систем (например, Kaspersky Mobile Security от Лаборатории Касперского).

Это интересно знать.

Большинство современных вредоносных программ для мобильных устройств (в основном это троянские программы) распространяются через Интернет под видом полезных программ (игр, кодеков для видеопроигрывателей и других), либо локально в людных местах посредством bluetooth. При этом установка вредоносной программы должна быть подтверждена пользователем.

Для защиты от таких вирусов следует соблюдать разумную осторожность:

- не принимать запрос соединения по bluetooth от незнакомых людей;
- не устанавливать подозрительные программы из ненадежных источников.

Однако в перспективе, с ростом использования смартфонов и коммуникаторов для выхода в Интернет, вредоносные программы для мобильных устройств могут стать серьезной опасностью.

Ряд специально установленных скрытно от владельца телефона (смартфона) вредоносных программ могут исполнять **шпионскую функцию**. Рассмотрим их подробнее.

Что такое шпионские программы для средств мобильной телефонной связи

Настоящее шпионские программы должны обладать чертáми, характерными для шпионов-людей: незаметно следить, замечать мельчайшие детали, добывать ценную информацию, действовать оперативно и скрывать малейшие следы своего присутствия.

Уникальные **шпионские программы для мобильных телефонов**, созданные экспертами в области информационной безопасности, подходят для установки на различные модели смартфонов с наиболее распространенными на сегодняшний день мобильными операционными системами: Windows Mobile, Symbian и iPhone OS.

В настоящий момент специалисты осуществляют также разработку лучших мобильных шпионов и перехватчиков под операционные системы Android и Maemo, набирающие все большую популярность.

Шпионские программы для мобильного телефона **базового уровня** способны следить и частично контролировать активность на мобильном устройстве, на которое они установлены. В результате вам будут доступны для просмотра в любое время суток даже в противоположной точке земного шара:

- текстовые сообщения, набираемые на телефоне;
- входящие и исходящие вызовы вместе с продолжительностью звонка;
- SMS, MMS, электронная почта;
- любые данные, полученные или переданные через Интернет;
- координаты мобильного телефона с точностью в несколько метров.

Помимо перечисленных функций **лучшие шпионские программы:**

- прослушивают и записывают все разговоры через мобильное устройство;

- могут превратить телефон в настоящий электронный жучок, прослушивая окружение, даже когда телефон находится в режиме ожидания.

Шпионская программа для телефона компактна, удобна в установке и использовании. Такую программу не волнуют такие мелочи, как смена SIM-карты. Она продолжает незаметную передачу данных в любых условиях.

Шпионские программы для телефона воспрепятствуют, например, общению ваших детей с людьми, связь с которыми, по вашему мнению, является для них нежелательной.

Это интересно знать.
Подобные программы можно также использовать на предприятии в случае необходимости слежения за временем пребывания сотрудников в офисе, а также за выполнением ими назначенных звонков.

Украсть телефон с установленным мобильным «шпионом» стало значительно сложнее. Ведь этот телефон продолжает передачу данных о своем местонахождении на сервера компании, которая продала вам соответствующую шпионскую программу. При этом протоколируется информация обо всех совершаемых звонках и передаваемых сообщениях, замечается любая активность злоумышленника на украденном телефоне.

Шпионские программы для мобильных телефонов помогут сохранить важную информацию даже в случае потери или кражи мобильного телефона, заблокировав смартфон в случае необходимости, а также помогут поймать злоумышленника.

Рассмотрим для примера некоторые шпионские программы для мобильных телефонов.

Возможности программы по прослушиванию окружения сотовых GSM телефонов Spy Phone Suite

Будьте осторожны.
Скачивая и устанавливая Spy Phone Suite, вы подтверждаете, что программа не будет использована способом, нарушающим текущее законодательство. Установка Spy Phone Suite на телефон другого лица без его ведома, перехват звонков и SMS сообщений может нарушать законодательство. Spyline.ru не несет ответственно-

сти за несоответствующее использование программы Spy Phone Suite. Приобретая годовую лицензию на использование и скачивая Spy Phone Suite, вы соглашаетесь с вышесказанным.

Программа обеспечивает полный контроль над любым лицом, имеющим мобильный телефон-шпион. Сопоставляя данные, полученные с помощью перехвата SMS сообщений, журнала вызовов и прослушки разговоров по сотовому телефону-шпиону можно без труда составить подробную картину того, куда, зачем, во сколько, с кем и для чего человек, носящий с собой телефон-шпион, ходит и делает.

Это интересно знать.
Эта программа способна контролировать коммуникации лица, на чей телефон установлена.

Она делает из телефона настоящий GSM-жучок, можете звонить на него и он, незаметно для владельца, будет прослушивать все, что происходит вокруг. Помимо функций по прослушке сотовых телефонов (их окружения) эта программа способна вести перехват всех SMS сообщений. Вне зависимости, входящие ли эти SMS или их пишет владелец телефона-шпиона. Любой текст, в любом формате, время отправки/принятия, телефон отправителя/получателя — все это будет доступно вам.

Если владелец телефона-шпиона будет пользоваться встроенным e-mail-клиентом, программа будет полностью дублировать вам его переписку и входящую корреспонденцию.

Так же программа, позволяет отображать координаты подконтрольного телефона (Location), посредством фиксации ID сотовых станций, в зоне которых он находиться в настоящий момент.

В программе ведется полная история всех входящих/исходящих вызовов, с записями времени звонков, их продолжительности. Если номер занесен в записную книжку телефона-шпиона, отобразиться не только его номер, но и имя контакта.

Программа по прослушке сотовых телефонов GSM и перехвату данных (SMS, e-mail) работает в скрытом режиме, она записывается в системном ядре и обнаружить ее практически невозможно.

Установка программы занимает не более 10 мин. Она доставляется по электронной почте в течение 24 часов с момента поступления средств продавцу программных продуктов.

Это интересно знать.

Все статистически важные данные (перехваченные SMS, E-mail, Location, история вызовов и пр.) передаются на ваш аккуант в WEBe и доступны вам 24 часа в сутки с любого компьютера/ноутбука или телефона с поддержкой HTML.

Существует несколько версий программы Spy Phone Suite (подробности см. на www.spyline.ru). Они приведены в **табл. 3.1.**

Возможности версий программы Spy Phone Suite *Таблица 3.1*

Функция/ Версия	Advanced	Standart	Basic	Audio	Audio Plus
Прослушивание разговоров по сотовому телефону	✓				✓
Использование телефона в качестве жучка	✓	✓		✓	✓
Перехват SMS/E-mail/Журнала звонков	✓	✓	✓		
Просмотр перехваченных данных через Интернет	✓	✓	✓		
Отслеживание через GPS	✓				
Уведомление о смене SIM-карты	✓	✓	✓		

На сайте разработчика www.spyline.ru можно скачивать **тестовую версию программы**. Тестовая версия программы по функциям идентична версии Advanced (Standart для Iphone), но ограничена по сроку действия до 48 часов.

Кроме того на сайте есть тестовая версия программы Spy Phone Suite для ознакомления с функционалом программы и проверки на совместимость с определенной моделью мобильного телефона.

Будьте осторожны.

*Программа работает с телефонами под управлением ОС Windows Mobile, IPhone OS или Symbian. При заказе в поле «Дополнительные сведения» **обязательно нужно указывать модель телефона**, на который вы собираетесь устанавливать программу. Не на все телефоны эта (и другие) программа может быть установлена.*

Варианты использования программы Spy Phone Suite

Рассмотрим основные направления для применения такого качественного решения по шпионажу.

Защита детей. Обезопасить собственного ребенка, не подвергая при этом его жизнь лишним ограничениям и неприятными разговорами — мечта любого родителя. Для того чтобы знать, что ребенок цел и невредим, что в круге его знакомых и друзей нет наркоманов, способных сбить с пути — достаточно просто время от времени прослушивать сотовый телефон, подаренный вами же.

А если вдруг чадо задержится, как он утверждает, в библиотеке после 12 ночи, всегда можно проверить его местоположение по спутнику с точностью до 10 м. В какую бы переделку ребенок не угодил, вы всегда будете знать, где он. Данное решение позволяет по-новому взглянуть на воспитание, без пустых подозрений и упреков вперемешку с постоянным страхом, что ребенок попадет в дурную компанию.

Деловые контакты. С помощью данного мобильного решения для прослушки сотового телефона и перехвата данных перед вами открываются по-настоящему безграничные возможности. Если вы — руководитель, в ваших руках оказывается полный контроль над подчиненными.

Узнать компетентность сотрудника или его лояльность — не уходят ли конфиденциальные сведения компании конкурентам или, быть может, сам нерадивый сотрудник использует их в личных интересах? Нет ничего проще. Во время ключевых переговоров подключаемся из любой точки планеты к разговору и прослушиваем беседу, не доступную вашему слуху прежде.

Даже для рядового сотрудника подобное мобильное решение является незаменимым для самого широкого круга задач, призванных максимально эффективно следовать вашим интересам: начиная от прослушивания мобильных телефонов руководства, коллег и заканчивая скрытым слежением за перемещениями интересующих лиц.

Семейная безопасность. Жизнь, особенно семейная, не всегда несет праздник. В сложное время некоторые супруги предпочитают искать утешение на стороне, подвергая унижению и обману своего мужа/жену. Благодаря программе для слежения/прослушке сотовых телефонов вы всегда будете знать о супруге: где он находиться, с кем и когда созванивается, о чем говорит, а также перехватывать любые SMS сообщения и e-mail-письма. В общем — вести полный контроль для точного выявления ненадежного человека.

Методика установки и использования программы Spy Phone Suite

Программное решение хорошо проработано. Установка программы занимает не больше 5 мин. и не требует никаких дополнительных подключений внешних устройств. Проще говоря: «скачал-настроил-забыл». После этого можно неограниченное время получать все данные в самой развернутой и подробной форме с любого компьютера (телефона), подключенного к сети Интернет.

Вся активность абонента будет перед вами как на ладони: перехваченные SMS сообщения, e-mail корреспонденция, журнал вызовов и даже координаты телефона, где бы он не находился на планете.

Вы можете прослушивать его сотовый телефон, как свой собственный, слушать, где он находиться, с кем ведутся переговоры или простая болтовня. А главное — с помощью этой программы вы сможете вести скрытую прослушку мобильных GSM диапазона, отмечается на **www.spyline.ru**. В любое время и в любом месте все коммуникации наблюдаемого лица будут под вашим полным контролем.

Это интересно знать.
Если вы пожелаете сменить телефон для прослушки — это можно сделать, не приобретая дополнительной копии программы.

Программа Spy Phone Suite в вопросах и ответах

Вопрос: *Как работает эта программа?*

Схематическое представление работы программы представлено на **рис. 3.1**.

Этап 1. На телефон, который следует прослушать, устанавливается программное обеспечение Spy Phone Suite. Это происходит через скачивание исполняемого файла на телефон и не требует ничего кроме самого аппарата и подключенной услуги GPRS.

Этап 2. После настроек и активации программы мобильный телефон (который следует прослушивать) возвращается владельцу.

Этап 3. Мобильный телефон с установленной программой в скрытом режиме передает на сервер в Интернет: тексты всех SMS, ведет перехват e-mail сообщений, а также журнал всех входящих и исходящих вызовов, координаты со спутника (если на телефоне есть GPS). Это позволяет с любого компьютера вести слежку за всеми коммуникациями целевого абонента.

Рис. 3.1. Схематическое представление работы программы Spy Phone Suite

Этап 4. Если на телефоне установлена версия Standart или Audio: сторонний телефон, чей номер был предварительно записан в программе, может звонить на телефон целевого абонента и прослушивать все происходящее вокруг. Если на телефоне установлена версия Advanced или Audio Plus. Помимо функции версии Standart (Audio), можно вести прослушку разговоров во время разговора целевого абонента с любым другим лицом.

Вопрос: *Как эта программа себя выдает?*

Программа по прослушке мобильных телефонов себя никак визуально не выдает. После установки она постоянно работает в фоновом режиме. Поэтому обнаружить ее в файловой системе или списке программ невозможно. Запустить программу на телефоне возможно только зная ключ активации, никак иначе.

Вопрос: *Будет ли работать программа по прослушке сотовых телефонов с любым КПК/телефоном?*

Программа работает на сотовых телефонах под управлением операционных систем Windows Mobile 5, Windows Mobile 6, Symbian 8.1, Symbian 9 и некоторых других, также на iPhone 2G/3G. Для того чтобы определить, будет ли работать определенный сотовый телефон с программой прослушки — необходимо воспользоваться специальной **таблицей совместимости, имеемой на сайте www.spyline.ru**. Если не удалось найти модель вашего телефона в таблице или вы не знаете

на какой операционной системе он работает, обратитесь в обратную связь этого сайта. Там помогут.

Вопрос. *Может ли абонент прослушиваемого телефона узнать о наличии программы по прослушке/перехвату данных через быстрое снятие средств с баланса за передачу секретных данных на сервер?*

Это маловероятно, поскольку сеансы передачи данных длятся меньше минуты и трафик расходуется минимальный, никаких видимых финансовых издержек абонент телефона-шпиона не понесет.

Вопрос. *Что мне делать, если программа не подошла к моему телефону/КПК или я просто желаю вернуть ее обратно?*

В случае, если по какой-либо причине программа покупателя не устроила, производители готовы инициировать процедуру возврата (отзыва) лицензии с возмещением затрат на покупку в установленной форме. Важно понимать, что производители дают гарантию корректной и качественной работы этого уникального программного обеспечения и готовы всегда пойти навстречу их клиентам.

Вопрос. *Скажите, безопасно ли хранятся данные на сервере производителей программы в интернете?*

Вся информация доступна только лицу, купившему продукт на сайте производителя. Ведь полностью автоматизирован процесс выдачи секретных данных с одной стороны и шифрования конфиденциальных данных с другой стороны.

Проще говоря, поскольку ни у кого, кроме данного покупателя, не будет логина/пароля/номера лицензии, никто не сможет узнать конфиденциальные данные на сайте. А поскольку на сервере вся информация храниться в зашифрованном виде — никто из сторонних или внутренних лиц не будет иметь к ним доступ.

Единственное слабое место — путь между ПК покупателя программы и сервером. Тут рекомендуется принимать стандартные меры предосторожности: не сохранять пароли, использовать firewall и антивирусное ПО.

Вопрос: *Как именно работает передача координат при наличии в телефоне GPS ?*

В ряде мобильных телефонов есть GPS приемник, получающий координаты со спутника и показывающий их на экране в виде цифр или, если есть привязка к карте, точек на карте. После установки на

телефон программы Spy Phone Suite по прослушке сотовых телефонов, нужно настроить ее на скрытую передачу этих данных (координат) на удаленный сервер (в Интернет).

Следует задать, как часто нужно эти координаты передавать — например, каждую минуту или 4 раза в день. После чего, программа в скрытом режиме будет передавать в Интернет координаты местоположения телефона. Заходите на специальный сайт, смотрите координаты.

Если хотите, можете нанести маршрут движения объекта на карту, например Google maps. Это очень удобно. Если в контрольный срок «снятия» данных GSM-сеть недоступна (выключен телефон или абонент в метро), координаты GPS сохраняются в буфер, и будут переданы на сервер, как только абонент войдет в зону доступа.

Вопрос. *Что такое «Location» и как использовать данные для получения информации о местоположении?*

Действительно, в программах SPS Advanced и SPS Iphone реализована подобная опция. Пункт «Location» в настройках программы активирует передачу данных о местоположении сотовой вышки, с которой в настоящий момент связан целевой телефон. Иными словами, вы получаете данные о том, где приблизительно находиться целевой телефон в определенный момент времени.

После активации данной опции в настройках программы, на сервер будут передаваться ID сотовых вышек. На странице сервера вы увидите следующие данные:

- имя оператора;
- ID (номер, идентификатор) сотовой вышки;
- код региона.

Используя данные сторонних ресурсов (netmonitor.ru) и баз сотовых вышек интересующего сотового оператора, которые могут быть загружены из сети Интернет, вы получите координаты исходных вышек и, как следствие, примерные координаты телефона.

Вопрос. *Можно ли использовать одну лицензию программы Spy Phone Suite на разных телефонах?*

Лицензию одновременно можно использовать **только на одном телефоне**. То есть, если пользователю программы стали не нужны данные на одном телефоне-шпионе, можно деактивировать программу и заново установить ее на другой телефон, который пользователь пожелает прослушивать/перехватывать данные.

Для деактивации нужно взять телефон, на котором установлена программа, выбрать пункт Deactivate и набрать код авторизации (выдается при покупке) Тем самым, мы деактивируем программу. После чего, программу можно установить на другой телефон, как это подробно описано в руководстве.

Вопрос. *Каким образом я смогу дозваниваться до абонента, если я его же и прослушиваю?*

Никак. Если вы записали свой номер в Call-лист программы, чтобы прослушивать телефон целевого абонента, то ваш звонок будет всегда проходить незаметно для владельца телефона. Поэтому желательно завести специальный номер, с которого вы будете прослушивать абонента и записать его в Call-лист, а для обычной коммуникации с абонентом использовать обычный номер.

Вопрос. *Если произойдет смена SIM-карты на целевом телефоне, как это отразится на работе программы?*

При смене сим-карты, на телефон слежения прийдет SMS-уведомление о смене карты с ее технической характеристикой. Программа устанавливается во внутреннюю память телефона и смена сим-карты никак не влияет на качество ее работы. Однако, для корректной передачи данных необходимо, чтобы на новой сим-карте был настроен и подключен GPRS.

Вопрос. *У меня не проходит установка программы, выдается ошибка, связанная со сроком действия сертификата. В чем может быть проблема?*

Проблема в некорректной установке даты на целевом телефоне, на который устанавливается программа. Исправьте дату на текущую и повторите попытку.

FlexiSpy: программа для прослушивания

Компания Vervata (http://www.flexi-spy.ru/) также предлагает решение для сбора информации с мобильного телефона человека, которого вы хотите проконтролировать. Она скрытно работает на телефоне в фоновом режиме и перехватывает информацию о входящих и исходящих звонках, тексты SMS и почты и местоположение телефона. Затем информация передается по каналу GPRS (через Интернет) на наш сер-

вер, где будет доступна вам с любого компьютера, подключенного к сети Интернет.

Также есть возможность включить микрофон наблюдаемого телефона и прослушать звуки, которые он улавливает, с другого телефона. Информация в этом случае передается по обычному аудиоканалу.

Чтобы установить программу, вам потребуется однократный кратковременный доступ (5—10 мин.) к телефону интересующего вас человека.

На сегодня FlexiSpy является одной из лучших программ такого рода. Программа приобрела широкую известность. Например, по данным Google, слово «FlexiSpy» повторяется в интернете 787 тысяч раз.

Существует два варианта программы — **FlexiSpy Light** и **FlexiSpy Pro**. Кроме этого, на сайте http://www.flexi-spy.ru/ предлагается:

- **программа Alert,** предназначенная для предотвращения утечки конфиденциальной информации в случае кражи или утери вашего телефона;
- **программа Bug,** предназначенная только для прослушивания аудиоинформации с микрофона наблюдаемого телефона. Возможности этих программ представлены в **табл. 3.2.**

Возможности версий программы компании Vervata *Таблица 3.2*

Возможности программ	Light	Pro	Alert	Bug
Перехват SMS	✓	✓	–	–
Перехват E-mail	✓	✓	–	–
Определение местоположения телефона	✓	✓	–	–
Перехват истории звонков	✓	✓	–	–
Прослушивание звуков, улавливаемых микрофоном	–	✓	–	✓
Защита частной информации при краже телефона	–	–	✓	–
Стоимость программы	100 евро в год	150 евро в год	50 евро одноразово	100 евро одноразово

Программы могут быть установлены только на модели смартфонов, работающие под управлением Symbian8, Symbian9, BlackBerry или Windows Mobile, указанные **на сайте компании Vervata.** Проверить, возможность установки данной выбранной программы на интересующую вас модель телефона нужно в меню «Телефоны».

Физический доступ к телефону для инсталляции программы. Предлагаемые программы не являются вирусами или троянами.

Следовательно, программа не может быть установлена дистанционно. Процесс инсталляции занимает около 5—10 мин. После завершения инсталляции физический доступ к наблюдаемому телефону не требуется.

Работоспособный канал GPRS абсолютно необходим для инсталляции. После инсталляции канал GPRS необходим программам Light и Pro для передачи перехваченной информации на удаленный сервер. Если соединение GPRS недоступно какое-то время, информация накапливается в наблюдаемом телефоне и будет передана на удаленный сервер при возобновлении соединения.

Соединение WAP не может быть использовано ни для инсталляции, ни для передачи информации. Функция «прослушивание аудиоинформации с микрофона наблюдаемого телефона» не требует соединения GPRS.

Необходим так же доступ к одному из средств оплаты: WebMoney, PayPal, VISA, MasterCard, American Express.

3.2. Защита мобильной связи от прослушки и слежения

Откуда у мобилки появились шпионские возможности

Сегодня мало кто не слышал о программах по прослушке сотовых телефонов. Эти программы-шпионы позволяют скрыто перехватывать ваши SMS-сообщения, узнавать суть ваших разговоров по телефону и даже в любой момент знать ваше местоположение.

Будьте осторожны.
*Всего за несколько тысяч рублей любой человек **может подвергнуть тотальному контролю любого,** во имя лишь собственных интересов.*

Прямо на наших глазах начинает разгораться бум с прослушиванием и даже более «подглядыванием» наших мобильных телефонов. И оказывается, чем круче мобильный телефон, тем больше шпионских функций можно задействовать:

- визуальное фотографирование окружающих лиц и предметов;
- видеосъемку и акустический контроль в радиусе до 10 м от мобильного телефона с последующей регистрацией всех говорящих;
- прослушивание всех входящих и исходящих телефонных разговоров, SMS и электронной почты и скрупулезная архивация всей информации;
- четко определять местоположение объекта (мобильника) с точностью до несколько метров;
- дистанционное включение микрофона с расстояния в десятки тысяч километров;
- дистанционное прослушивание разговоров через микрофон телефона, даже если основная батарея вынута (для современных SMART телефонов).

Естественно, что данные технологии контроля над мобильными телефонами использовались ранее только западными **спецслужбами** в рамках борьбы с террористами и криминальными элементами. В России разработки и производства мобильных телефонов до настоящего времени не было.

При производстве простых мобильных телефонов указанные функции были реализованы на аппаратном уровне. Они активизировались только по специальным запросам, которые были известны соответствующим западным спецслужбам. Данные мероприятия осуществлялись в рамках законодательства своих стран.

При развитии технологии мобильной связи и появлением SMART телефонов и коммуникаторов, соединяющих функции телефона и компьютера реализация «специальных» функций или как их называют «полицейских» легла и на операционные системы, которые используются в мобильных технологиях.

Все труднее стало производить универсальные высокоскоростные экономичные процессоры для мобильных телефонов, которые реализуют еще дополнительную «полицейскую» функцию.

Это интересно знать.

Такое значительное перераспределение специальных функций ***с аппаратной части на программную*** *привела к тому, что опытные программисты стали ее ловко использовать. Был создан целый ряд так называемых* ***«spy» (шпионских) телефонов*** *на базе серийно выпускаемых мобильных телефонов.*

Насчитывается более 70 моделей известнейших в мире производителей мобильных телефонов, таких как NOKIA, SIEMENS, PANASONIC, MOTOROLA, SAMSUNG, SONY-ERICSSON и других, на базе которых были разработаны «spy» телефоны.

Ложные базовые станции

Для программистов стало возможным создание недорогих ложных базовых станций (таких как **«ловушки» IMSI**). Эти станции занимаются активацией микрофона на вашем мобильнике с помощью ложных звонков или SMS.

Например, в информации о новой услуге ложного оператора, совсем не примечательной на первый взгляд, может содержаться код активации микрофона вашего мобильника для последующего прослушивания разговора и помещения.

Определить, что включился ваш микрофон практически очень сложно, и злоумышленник спокойно может слышать и записывать не только ваши разговоры по телефону, но и разговоры в помещении, где находиться мобильный телефон.

Это интересно знать.
Это, в основном, характерно для современных коммуникаторов и SMART телефонов.

Таким образом, к вашему мобильному телефону очень престижному и элегантному совершенно спокойно могут подключиться не только спецслужбы (естественно в соответствии с законом), но и большое количество конкурентов с целью получения сведений о вас, в том числе, и компромата.

Можно ожидать появления огромного числа «spy» телефонов. Главное, что номенклатура их с каждым днем расширяется.

Будьте осторожны.
Теперь мы не можем точно знать, какой телефон мы покупаем: обычный или «spy» и какой телефон нам вернут после незначительного ремонта.

Производители телефонов ни в коей мере юридически не отвечают за эти достаточно странные изменения. Не было ни одного официаль-

ного заявления ни NOKIA, ни SIEMENS о том, что нельзя использовать свои телефоны как подслушивающие устройства, что это нарушает права человека.

Антишпионское программное обеспечение

Для поиска и уничножения программ-шпионов в вашем мобильном телефоне появилось специальное антишпионское программное обеспечение.

Ведь ни один антивирус для мобильных телефонов Nokia, Samsung и других популярных моделей **не мог до сего момента защитить** от этой угрозы. В том числе такие известные приложения, как kaspersky mobile security и norton smartphone security.

Благодаря лишь антишпиону для телефонов Spy Monitor Pro, который можно скачать на сайте www.spyline.ru, ситуация в корне переменилась. Этот новейший мобильный антитроян — **единственная защита** от многочисленных программ-шпионов.

Программа Spy Monitor Pro

Программа «антишпион / антитроян» способна гарантированно ловить любые шпионские приложения для телефонов GSM/3G. Разработчик **Spy Monitor Pro** гарантирует возможность нахождения и удаления любых шпионских приложений для мобильных телефонов.

Spy Monitor Pro — это антитроян, который ловит любые шпионские приложения на мобильных телефонах. Необходимо скачать этот антишпион для своей Nokia или другой модели. Затем можете начать немедленное сканированное системы и/или поставить в настройках регулярное фоновое сканирование телефона на предмет наличия шпионов/троянов.

После обнаружения вредоносного ПО, антитроян Spy Monitor **предложит безопасно для системы удалить** несанкционированное программное обеспечение. Удалению подвергаются все шпионские приложения, даже с дополнительными параметрами защиты от удаления.

Версию антитрояна Spy Monitor Pro отличает расширенный функционал и **годовая лицензия** на использование. Существует бесплатное обновление антишпионской базы.

Благодаря гибким настройкам и интуитивно понятному интерфейсу этот мобильный антишпион для Symbian 9-й серии **прост и удобен** в использовании. А благодаря совершенной системе распозна-

ния шпионских сигнатур в совокупности в широким мониторингом вы всегда можете быть уверенны **в полной защите от прослушки.** Все что для этого нужно, это скачать программу антишпион Spy Monitor.

Данная версия антитрояна: Spy Monitor Pro, предназначена **для постоянного сканирования телефона** на наличие вирусов/троянов с возможностью удаления несанкционированного ПО. Как в интерфейсе программы, так и в фоновом режиме. **Спецификация такова.**

- Срок действия лицензии — **1 год.**
- Совместимость: Телефоны на базе **Symbian 9** (полный список моделей см. на www.spyline.ru) и **Windows Mobile 5,6 и выше** (все модели).
- Сканирование памяти телефона по запросу пользователя.
- Выполнение функции антивируса для телефона — предупреждение о установленных шпионских приложениях.
- Удаление любого найденного вредоносного приложения из меню Spy Monitor Pro.
- Установка программы занимает не более 5 мин. и она доставляется по электронной почте в течение 24 часов с момента поступления средств.
- Возможность сканирования в фоновом режиме.
- Автообновление антишпионской базы.
- Гарантия нахождения любого шпионского приложения.

Видео и текстовая инструкции по установке и эксплуатации для Symbian 9 и Windows Mobile 5,6 и выше доступны на сайте www.spyline.ru. Там же есть подробная инструкция по установке для Symbian 9 и Windows Mobile 5,6 и выше в формате PDF.

Поддержка моделей:

- все телефоны на базе операционной системы Symbian 9 третьего поколения и выше;
- все телефоны на базе операционной системы Windows Mobile 5,6 версий и выше.

Перед покупкой программы рекомендуется уточнить совместимость Spy Monitor — антивируса для мобильных телефонов у **специалиста службы поддержки.**

Специальные антишпионские телефоны

Использование **специально разработанных телефонов существенно более дорогое решение этого вопроса.** Они имеют встроен-

ные системы контроля аппаратных и программных средств, исключают возможность любого вида несанкционированного съема информации.

Это позволит вам избежать прослушивания со стороны конкурентов. На современном коммерческом рынке присутствуют многочисленные производители крипто GSM, которые можно разделить на категории, хотя они имеют общий подход к решению задачи: они созданы на базе серийно выпускаемых GSM телефонов.

Аппаратную реализацию шифрования в GSM телефоне также можно разделить на два подхода:

- дополнительный чип внутри GSM телефона;
- дополнительное устройство, выполняющее функцию шифрования, которое подсоединяется к обычному GSM телефону.

Другой подход — это программное шифрование речи с помощью процессора, который имеется в GSM телефоне.

Очевидно, что оба метода имеют существенные недостатки в области защиты от излучений микрофона GSM и других высокоизлучающих компонентов, гармоники которого свободно выходят в эфир через антенну GSM, и могут быть перехвачены недорогим сканером на расстоянии десятков километров.

Нет необходимости использовать самые сложные алгоритмы шифрования: открытая речь присутствует в эфире. В свою очередь программные шифраторы имеют существенный недостаток: ключи хранятся на процессоре, который непосредственно подключен к модему телефона. Украсть ключи не составляет большого труда.

Это похоже на то, что человек запирает машину на замок и кладет ключи рядом с ней и при этом доказывает, что защита машины супер отличная. Это актуально, потому что программные системы шифрования GSM используют операционную систему Windows, которая часто подвергается атакам многочисленных вирусов, в том числе так называемых «троянских коней».

Криптосмартфон ANCORT A-7

Производитель специализированных телефонов должен вам предоставить гарантии, что телефон невозможно прослушать, и что в нем нет систем удаленного включения микрофона.

Компания «АНКОРТ» отмечает на своем сайте, что может дать указанные гарантии. Обо всех технических деталях защиты крипто

смартфона смотрите на сайте компании. Для примера рассмотрим **криптосмартфон ANCORT A-7**

Криптосмартфон Ancort полностью разработан компанией «АНКОРТ» и не использует GSM платформы сторонних производителей. Стоимость разработки криптосмартфона и его специальных исследований составляет около 1 млн.

Криптосмартфон ANCORT A-7 изначально планировался для криптографической защиты. В телефоне имеется специализированный крипто чип, специальные фильтры и металлический экран, которые предотвращают опасные излучения. В криптосмартфоне отсутствуют такие высоко излучающие элементы, как видеокамера, Bluetooth, инфракрасный порт, съемная дополнительная память, Wi-Fi.

Кроме того, разработана уникальная система контроля правильности работы шифратора. Реализация особой системы синхронизации обеспечивает надежную работу криптосмартфона в роуминге, особенно тогда, когда роуминг приходится осуществлять на значительно удаленные расстояния, где при передаче используются аналоговые средства передачи данных.

В этом случае в криптосмартфоне разработана уникальная система восстановления криптосинхронизации, что обеспечивает высокую надежность соединения.

Криптосмартфон ANCORT A-7 имеет высочайшие криптографические, инженерно- криптографические характеристики, что обеспечивают надежную криптографическую защиту.

Шифрование SMS и E-mail. В ANCORT A-7 впервые реализована полноценное шифрование текстовых сообщений, передающихся по каналам связи протокола GSM.

Исключение возможности атаки «Человек в середине». Атакой «человек в середине» называется такой тип атаки, когда атакующий получает возможность читать, добавлять и изменять по своему желанию сообщения и другую информацию. Причем ни один из собеседников знать об этом не будет. Атакующий должен иметь возможность отслеживать и перехватывать сообщения (информацию) между собеседниками. Такая атака становится возможной при использовании обмена ключами по Diffie-Hellman, если обмен ключами происходит без идентификации (проверки подлинности источника).

Криптосмартфон Анкорт использует встроенные алгоритмы и уникальную систему идентификации звонящего, что, в свою очередь, исключает возможность атаки «человек в середине».

Защита от вирусов, которые позволяют прослушивать телефон абонента, с помощью любого другого телефона или специализированного компьютера. Для защиты от данного типа вирусов при разработке криптосмартфона была разработана дополнительная аппаратная часть, которая позволяет избежать действия этих вирусов на эффект несанкционированного прослушивания разговора с других мобильных телефонов и в непосредственной близости от него.

Защита от незаявленных возможностей. При разработке Криптосмартфона Ancort, были проведены необходимые исследования, в результате чего была разработана специальная аппаратная часть криптосмартфона, не допускающая несанкционированного прослушивания и удаленного включения микрофона. Этим криптосмартфон Ancort отличается от других смартфонов известных производителей, в которые только устанавливается программа шифрования, а другие способы защиты отсутствуют.

Защита от наводок. Во многих современных сотовых телефонах и даже криптофонах излучения микрофона GSM и других высокоизлучающих компонентов, гармоники которых свободно выходят в эфир через антенну GSM, и могут быть перехвачены недорогим сканером на расстоянии десятков километров. ANCORT A-7 защищен от устройств позволяющих прослушивать стандартные GSM телефоны. С целью повышения защиты на телефон были установлены специальные экраны и фильтры.

Защита от утечки информации в результате утери, хищения, получения временного доступа. Расшифровать ранее зашифрованную информацию невозможно, даже если вашим телефоном завладели (утеря, кража, получили временный доступ). Потому, что для каждого сеанса связи создается временный «сеансовый ключ», который в дальнейшем невозможно восстановить. Это обеспечивает сохранность разговоров, зашифрованных SMS и E-mail, даже если телефон был утерян.

Низкое время задержки в крипто режиме. Задержка составляет около 0,7 с. Из них 0,5 с составляет задержка по причине низкого приоритета канала передачи данных, а оставшиеся 0,2 с занимает процесс шифрования. Задержка при обычном разговоре в сети GSM равна 0,08 с. В любом случае, если вы разговариваете, находясь на некотором расстоянии от собеседника, задержка не заметна.

Высокое качество речи в крипто режиме. Слоговая разборчивость составляет 87%. Это соответствует высокому показателю качества,

находящегося на уровне коммерческого. В мире не существует аналогичного шифратора с таким уровнем качества разговора в шифрованном режиме.

Возможность синхронизации с компьютером. Для этого необходимо установить Microsoft ActiveSync на ПК и подключить криптосмартфон к компьютеру, используя USB-кабель.

Простота использования. Установление защищенного соединения или передача защищенного текстового сообщения происходит нажатием одной кнопки.

Возможность использования по всему миру. Телефон проходил испытания более чем в 30 странах, в том числе во Франции, Швейцарии, Китае, Индии, Малайзии, Сингапуре, Арабских Эмиратах, Швеции, ЮАР.

Международное признание. ANCORT A-7 неоднократно участвовал в различных выставках проводимых по всему миру и показал свое неоспоримое превосходство над аналогичными изделиями таких известных брендов, как Rohde & Schwarz, GSMK CryptoPhone, Siemens и др.

Престижность. ANCORT A-7 используется для обеспечения безопасности первых лиц государства в таких странах, как ОАЭ, ЮАР, Сингапур и т. д. Так же известные и состоятельные люди всего мира доверяют свою безопасность ANCORT A-7.

Совместно с известнейшим в мире австрийским ювелиром, дизайнером и изобретателем роскошных мобильных телефонов, господином Петером Алоиссоном был разработан Бриллиантовый Криптосмартфон стоимостью 1.300.000 USD, специально для людей которым важно не только защитить свою информацию, но и подчеркнуть свою индивидуальность.

ANCORT A-7 не просто защитит вас от прослушивания, но и подчеркнет статус владельца! Стоимость базовой модели составляет около 3000 долларов.

Это интересно знать.

Для обеспечения надежной криптографической связи необходимо иметь минимум два криптосмартфона ANCORT A-7.

Зачем нужен криптосмартфон?

В настоящее время в мире используется более 500 000 000 GSM телефонов, по которым передается огромное количество совершенно раз-

личной информации — политической, финансовой, экономической, юридической, медицинской и личной. Использование этой информации криминальными элементами чрезвычайно опасно и может привести к катастрофическим последствиям, как для государства, корпораций так и для частных людей.

Проблема похищения людей (киднаппинг). Особенно этой угрозе подвержены дети богатых родителей. Преступники фальсифицируют голос родителей, говорящих по GSM телефону, и выманивают детей с целью их похищения. Доходы от киднаппинга составляют в мире колоссальную сумму, многие сотни миллионов долларов. Подделка голоса и речи — наиболее легкий и недорогой способ, облегчающий похищение людей.

Фальсификация голоса и смысла речи политических деятелей, говорящих по GSM, с последующей публикацией в прессе фальшивых разговоров с соответствующими комментариями. Правительства многих стран тратят сотни миллиардов долларов на оборону своих стран, но зачастую у них не находится никаких денег на защиту телефонных переговоров своих государственных деятелей, даже когда они работают за территорией своих стран, где их наиболее легко скомпрометировать.

Фальсификация голоса и речи деятелей шоу бизнеса с целью разворачивания криминальными папарацци шумной компании для компрометации и организации гонения на них. Чрезвычайно выгодна для криминальных папарацци и приносит им доходы во многие десятки миллионов долларов.

Нередки случаи использования перехваченной информации по GSM, касающейся болезни человека. Публичное разглашение медицинской тайны о болезнях пациента для устранения его с должности, особенно когда он занимает высокое положение.

Фальсификация разговоров религиозных деятелей с целью разжигания религиозных конфликтов.

Похищение корпоративных и личных конфиденциальных данных с целью разорения конкурентов. Большинство хакеров прослушивают мобильные телефоны и разговоры по ним, чтобы узнать пароли доступа к корпоративным базам данных и банковским счетам.

Использование личных сведений о людях для осуществления рэкета и вымогательства.

С технической точки зрения перехват GSM переговоров сравнительно несложен по следующим причинам.

Стоимость несанкционированного перехвата и записи телефонных переговоров по GSM сравнительно невысока и колеблется от 1000$ до 2000$ за запись одного номера GSM в течение месяца.

Размеры аппаратуры для перехвата — немного больше портативного компьютера. Ее легко переносить и перевозить. Обнаружить ее практически невозможно, это и есть так называемый «пассивный режим». Аппаратура одновременно может контролировать до 16 телефонных номеров GSM.

Стоимость компьютерного моделирования голоса человека, говорящего по GSM, немного выше. А последствия, можно себе представить, более разрушительны.

Громкий скандал с известнейшим певцом России Л. Агутиным, чей голос был подделан злоумышленниками, что привело к тому, что отец певца выплатил вымогателю 30000$.

ГЛАВА 4

УСТРОЙСТВА ПОИСКА ЖУЧКОВ И ЗАЩИТА ОТ ПРОСЛУШКИ

Противошпионские штучки, созданные для информационной защиты, помогут избежать утечки важнейшей информации. Как правило, информационная безопасность состоит из нескольких элементов: обнаружение источника считывания информации; определение круга лиц, кто мог установить шпионские штучки; дезинформация; отключение; уничтожение данных. Но лучше предупредить утечку информации с помощью индикаторов поля.

Почему возникла необходимость в антижучках

За последние годы в нашей стране продано скрытых камер и подслушивающих устройств на более чем 100 млн. долларов и эта цифра неуклонно растет. По фактам незаконного использования спецсредств и незаконной слежки возбуждено множество уголовных дел. Менеджеры высшего звена, крупные чиновники и руководители разного ранга лишились своих должностей из-за компроматов, полученных с помощью средств негласного наблюдения и/или записи переговоров.

Резкое уменьшение размеров жучков и активное использование их частными детективными агентствами в несколько раз за последний год увеличило число разводов, причиной которых стали видеосвидетельства измен супругов. Все большей популярностью пользуется шантаж на бытовом уровне, когда при минимальных затратах злоумышленник получает приличную компенсацию с людей, подчас не имеющих желания обратиться в правоохранительные органы. Жучки устанавливаются: в саунах, гостиницах, мотелях, офисах, в примерочных магазинов, в общественных туалетах, в раздевалках спортивных клубов, в косметических и врачебных кабинетах частных клиник. И это далеко не все места использования данных устройств.

Выбор случайного места для романтических встреч или проведения секретных переговоров, нахождение на нейтральной территории,

например, в сауне или в гостинице, тоже не гарантирует сохранение конфиденциальности. Миниатюрные жучки, передающие видео по радио или транслирующие ваши переговоры, могут быть установлены в любом помещении за несколько секунд.

Единственно, как можно узнать работу жучка — это по излучению, издаваемому передатчиком беспроводного устройства. Изображение или звук передаются с помощью электромагнитных волн на удаленный приемник. Именно это и улавливает карманный детектор жучков (индикатор поля). При помощи таких детекторов жучков в любом месте в любое время вы сможете быть уверены в том, что ваш разговор не слышит кто-то еще.

Обнаружители жучков имеют современный привлекательный дизайн, компактны, отдельные модели не менее миниатюрны, чем сами жучки. Несложное управление детекторов жучков позволит вам своевременно предотвратить запись ваших деловых переговоров, просто разговоров с кем-нибудь, телефонных или нет, в помещениях или вне их.

Таким образом, необходимость поиска жучков в наше время — проблема, с которой может столкнуться каждый гражданин. Это перестало быть задачей только агентов 007 и сотрудников правоохранительных служб.

Антижучки предназначены для сканирования и эффективного выявления жуков прослушки, подслушивающих и подглядывающих устройств (беспроводных видеокамер) работающих по радиоканалу. **Антижучки** — новейшие электронные приборы, умещающиеся в руке, не привлекающие внимания. Эффективность антижучков подтверждена десятками найденных прослушивающих устройств. Эффективность обнаружения подслушивающих устройств, жучков и беспроводных видеокамер 99%!

Рассмотрим компактные ПРОФЕССИОНАЛЬНЫЕ устройства поиска жучков, подслушивающих устройств и скрытых камер, **BugHunter** и другие.

Приборы серии BugHunter (антижучки) — заслуженно признанные устройства, гарантирующие профессиональный уровень работы. Детекторы жучков и скрытых камер BugHunter используются профессионалами.

Разработчик прибора — компания i4Technology, российское предприятие, зарекомендовавшее себя как успешную и надежную компанию по производству высококачественной продукции с длительным

сроком эксплуатации. BugHunter производится только российскими предприятиями — признанными лидерами в области систем безопасности. Устройства имеют соответствующие награды и признание среди российских структур обеспечения безопасности.

Совет.

Остерегайтесь подделок!!! К сожалению, большинство устройств-подделок для обнаружения электронных жучков создают лишь иллюзию безопасности и не способны в «боевых условиях» найти радиожучок или скрытую камеру, отмечается на ***http://antibug.com.ua****. Хорошего всегда мало! Профессионалы используют только профессиональную технику, а не игрушки!*

Profi BH-07 — антижучок профессиональный, детектор жучков и камер

Этот профессиональный антижучок (**рис. 4.1**) легкий в использовании, что позволит даже неподготовленному пользователю обезопасить себя от нежелательной утечки информации. Разработанное спецслужбами для использования в целях контршпионажа данное устройство поиска прослушки станет полезным везде, где пользователя могут подслушивать или скрыто снимать: залы заседаний, гостиничные номера, ванные комнаты, квартиры, офисы, автомобили, государственные учреждения.

Рис. 4.1. Внешний вид детектора жучков и камер Profi BH-07

Отличительной особенностью данной модели детектора жучков (обнаружителя камер) является диапазон сканируемых частот и дальность покрытия. Детектор прослушки имеет большой диапазон сканируемых частот: 1—8000 МГц и большую дальность покрытия — до 25 м.

Принцип работы детектора прослушки основан на приеме скрытых сигналов излучаемых аудио или видео закладками (жучками). Благодаря возможности регулирования уровня приема и силы сканируемых частот поисковик жучков и камер может обнаружить любые, даже самые малые жучки, телефонные перехватчики, микро видео камеры, радиозакладки и прочее.

Корпус прибора выполнен из высококачественного сплава, не излучающего помех, с мелко шлифовальным профилированным покрытием. Детектор не излучает электромагнитные волны и не вмешиваться в работу каких-либо электронных приборов, а также абсолютно безвреден для здоровья.

Также прибор можно использовать в бытовых целях для оценки наличия и уровня электромагнитного излучения в помещении. К примеру, при поломке микроволновой печки, электротехники, повреждении линий электропередач прибор обнаружит интенсивное электромагнитное излучение.

Технические характеристики:

- частоты поиска, МГц ..... 1—8000 ;
- чувствительность, мВ .. 0,05 (очень высокая чувствительность);
- динамический диапазон, Дб 70;
- дальность покрытия, м ..... до 2;
- режим работы ..... 10 уровней индикации с сопровождающимся звуковым и световым сигналом;
- источник питания ..... 9 В батарея;
- размеры (без антенны), мм..... 125×65×25;
- размеры (с антенной), мм.....280×65×25.

BugHunter-01 Профессиональный — детектор жучков и скрытых видеокамер наблюдения

BugHunter-01 Профессиональный (**рис. 4.2**) — уникальная российская разработка, которая потрясла своей технологичностью, точностью и чувствительностью весь рынок средств безопасности! Прибор предназначен для оперативного обнаружения и поиска жучков, радиоизлучающих устройств, радиозакладок, в том числе:

- радиомикрофонов, телефонных радиоретрансляторов;
- радиостетоскопов;
- скрытых видеокамер с передачей информации по радиоканалу;
- радиомаяков, систем слежения за перемещением объектов;
- несанкционированно включенных радиостанций и радиотелефонов.

***Рис. 4.2.** Внешний вид BugHunter-01 Профессиональный*

Это интересно знать.
Все китайские детекторы, и большая часть российских, доступная в свободной продаже, либо имеют провалы чувствительности в частотном диапазоне, либо резкое ее уменьшение.

Например, некоторые не обнаруживают излучение Wi-Fi, хотя заявлено, что работают до 3000 МГц, либо чувствительность на этом диапазоне близка к нулю. Провалы могут быть и не только на частоте 3000 МГц, но и на любом другом частотном промежутке.

Подавляющее большинство детекторов построено на высокочастотных диодах. Основной недостаток данной конструкции — узкий диапазон частот. Т. е. прибор хорошо детектирует сигнал, например, в диапазоне частот 300—600 МГц, в остальных — значительно хуже, либо вообще чувствительность практически нулевая. Таким образом, чувствительность у них на всем диапазоне частот не равномерная. Это приводит к тому, что эти детекторы «слепы» к жучкам, работающим на «проваленных» частотах. Хотя все производители заявляют, что их продукция работает на всем диапазоне, от 50 до 3000 МГц. Но это не соответствует действительности.

Обнаружитель жучков BugHunter Профессиональный BugHunter-01 охватывает весь возможный диапазон, на которых работают жучки, от 50 до 3000 МГц. Это достигается:

- специальным конструктивом (имеется как внутренняя, так и внешняя антенна для низких частот);
- специальной высокоскоростной элементной базой.

Реальная, действительная чувствительность прибора BugHunter Профессиональный — 50 мВ/м. Это значит, что радиозакладка или жучек мощностью 5 мВт будет обнаружен уже на расстоянии 5 м. А сотовый телефон — уже на 50 м! Это действительно уникальный результат.

Китайские детекторы радиозакладок и скрытых камер видеонаблюдения не выдерживают вообще никакой критики. Им характерны низкая чувствительность, не соответствие заявленным параметрам, провалы в частотных диапазонах. Китайские детекторы жучков можно рассматривать как игрушку, которая не может быть использована для серьезной работы.

Расширенный динамический диапазон. Уникально! Динамический диапазон детектора 45 дБ, в то время как у большинства остальных приборов российской разработки — не более 40 дБ. Это значит, что шкала чувствительности значительно шире. Т. е. прибор будет пока-

зывать как сигналы очень низкой мощности, так и сигналы очень высокой мощности. И при этом не выходить за пределы своей шкалы отображения. Расширенный динамический диапазон значительно повышает вероятность обнаружения жучков и любых других радиозакладок при сложных условиях поиска.

Обнаружение цифровых жучков (коротких импульсов)! Уникально! Существует вид жучков прослушки, которые работают **по цифровому принципу**, т. е. передают информацию как бы порциями, замолкая на некоторое время. Это позволяет им замаскироваться от большинства детекторов жучков российской и азиатской разработки. Они детекторы просто не в состоянии обнаружить цифровой сигнал. Это не удивительно, так как они разрабатывались для обнаружения жучков, постоянно излучающих электромагнитное поле (аналоговые жучки).

Обнаружитель жучков BugHunter Профессиональный BugHunter-01 специально спроектирован таким образом, чтобы обнаруживать как обычные аналоговые сигналы, так и цифровые.

Автоматическая подстройка под фоновый уровень излучения. Уникально! В любом городе множество источников излучения: сотовая связь, радиостанции и т. д. И в этом море шума необходимо выявить именно сигнал от жучка. В детекторе жучков BugHunter Профессиональный разработана **технология автоматической подстройки под фоновые шумы**. Это позволяет прибору не реагировать на фоновое (постороннее) излучение, а обнаруживать именно локально расположенный жучек. Функция является уникальной, потому что прибор производит подстройку автоматически. Т. е. можно спокойно проводить переговоры, в то время как детектор будет постоянно отслеживать обстановку и автоматически подстраиваться под фоновый уровень излучения. Как только включат жучок или любую другую радиозакладку, прибор BugHunter Профессиональный немедленно даст знать об этом. Другие детекторы не имеют такой полезной функции.

Возможность подключения наушников, скрытого предупреждения. Используя наушник, можно скрыто контролировать ситуацию, нет ли поблизости активированных жучков. При обнаружении жучка BugHunter BugHunter-01 сообщит об этом скрыто, звуковым сигналом через наушник. Можно вести переговоры и одновременно контролировать радиочастотную обстановку.

Световая сигнализация. Детектор радиозакладок BugHunter Профессиональный BugHunter-01 также может оповестить только световой сигнализацией (т. е. без звука). Например, прибор можно

положить на стол. Как только будет обнаружен источник излучения, детектор просигнализирует только световой сигнализацией.

Расширенный температурный режим работы. Высококачественная элементная база позволяет использовать BugHunter Профессиональный в экстремальных температурных режимах, от −30 °С до +80 °С. Другие подобные приборы не могут похвастаться способностью работать при таких экстремальных температурах. Детектор также сохраняет заданную чувствительность во всем этом диапазоне температур. В то время как у других на морозе или на жаре чувствительность падает.

Три режима работы прибора:

- **Поиск.** В режиме поиска прибор работает со световой и звуковой индикацией. Чем ближе прибор находится к источнику, тем выше уровень светового сигнала на шкале. Можно отрегулировать уровень чувствительности детектора. Если рядом мешают поиску сильные источники сигнала.
- **Охрана.** Режим охраны переводит детектор жучков в режим автоматической настройки чувствительности и низкого энергопотребления. Этот режим предназначен для постоянной фоновой работы. Детектор сам автоматически подстраивается под специфику радиообстановки. В режиме охраны, например, BugHunter Профессиональный можно носить с собой, можно проводить переговоры. Детектор периодически сканирует пространство на предмет радиоизлучений. При этом в зависимости от настроек может предупредить об обнаружении жучка как скрыто, так и звуковой/световой сигнализацией.
- **Режим акустозавязки.** Что такое акустозавязка? Когда кто-нибудь из радиослушателей звонит на радиостанцию и не выключает свой приемник, возникает «свист». Этот эффект возникает, когда микрофон находится рядом с динамиком, который воспроизводит то, что улавливает микрофон. Получается замкнутая цепочка: микрофон-динамик-микрофон-динамик-... Это слышится как «свист». Акустозавязка используется для поиска скрытых микрофонов (жучков), работающих в аналоговом режиме. Жучок улавливает звук детектора, передает его по радио, радио улавливает детектор и снова воспроизводит в виде звука. Цикл замыкается — и получается «свист». Режим акустозавязки позволяет наиболее точно обнаружить по характерному «свисту», где именно установлен жучек. Время поиска сокращается.

Увеличенная длительность работы. Расширенные функции энергосбережения. Охранный режим работает с максимальным энергосбережением, поэтому батарей питания хватает надолго.

Подстройка яркости свечения индикаторов в зависимости от разряда батареи.

Широкий диапазон напряжения питания. За счет преобразователя напряжения работает в диапазоне 1,8— 5 В. Таким образом, возможна работа как от обычных батареек, так и от аккумуляторов.

Индикация разряда батареи. Детектор сообщит о необходимости замены батарей питания;

Самодиагностика. Прибор автономно тестирует собственную работоспособность при включении. Это дает гарантию, что прибор работоспособен и действительно улавливает излучения жучков. В противном случае прибор выдаст сообщение о поломке.

Имеется возможность подключения **наушников** и дополнительная **внешняя антенна.**

Технические характеристики прибора:

- диапазон рабочих частот (это весь диапазон, на котором работают жучки и скрытые камеры), МГц. . .50—3000;
- чувствительность (минимально обнаруживаемая напряженность поля), не менее ..... 50 мВ/м (самая высокая чувствительность);
- динамический диапазон, дБ, не менее 45;
- дальность обнаружения радиопередатчика 5 мВт, м 5;
- дальность обнаружения сотового телефона, м.....50;
- габариты, мм .....105×58×18.

BugHunter-2 Профессиональный — детектор жучков и скрытых видеокамер

Долгожданная новинка! Вышла принципиально новая версия популярнейшего детектора жучков, беспроводных видеокамер и других шпионских закладок BugHunter Профессионал BugHunter-1. Новая версия детектора BugHunter-2 (**рис. 4.3**) может похвастаться увеличенным динамическим диапазоном (48 дБ вместо 45), в результате чего повысилась и без того высокая эффективность поиска жучков слежения. Еще одно новшество — встроенный GSM фильтр, гарантирующий качественную защиту от помех, вызываемых близко расположенными антеннами мобильной связи. В остальном функции

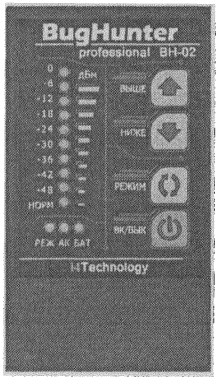


Рис. 4.3. Внешний вид BugHunter-02 Профессиональный

антижучка BugHunter-2 полностью идентичны модели BugHunter-1. Детектор жучков слежения BugHunter-2 идеально подходит для обнаружения цифровых и аналоговых шпионских закладок, радио и мобильных телефонов, беспроводных видеокамер, раций и других шпионских устройств в тяжелых условиях поиска.

Чем же BugHunter Профессионал BugHunter-2 отличается от предыдущей модели BugHunter-1?

Защита от GSM помех антенн мобильной связи. Каждый, кто хоть раз работал с детекторами жучков, знает, что GSM помехи это очень сильный фактор, который затрудняет поиск жучков и другой шпионской техники в черте города. Помехи от вышек мобильной связи заглушают и без того слабые сигналы жучков. В результате даже использование качественных антижучков с высокой чувствительностью становится невозможным: детекторы просто не могут идентифицировать сигнал жучков на фоне более мощных радиосигналов, заполняющих эфир. К счастью, новая модель BugHunter Профессионал BugHunter-2 лишена данного недостатка, т. к. оснащена специальным GSM фильтром, который автоматически блокирует помехи от антенн мобильной связи. GSM фильтр позволяет детектору жучков очень эффективно работать даже в сильно засоренном помехами эфире и прекрасно подходит для использования даже в непосредственной близости от базовых станций сотовой связи!

Увеличенный динамический диапазон. Динамический диапазон в модели BugHunter-2 составляет впечатляющие 48 дБ, в то время как у предыдущей модели (BugHunter-1) он 45 дБ, а у большинства аналогов — не более 40. Спектр чувствительности нового индикатора поля значительно шире. Это означает, что данный прибор может определять сигналы как очень низкой, так и очень высокой мощности, не выходя за пределы своей шкалы отображения. Другие детекторы жучков могут вообще не показать слишком слабый сигнал или же выйдут за пределы шкалы при очень сильном сигнале.

Расширенный динамический диапазон существенно уменьшает время поиска жучков и других радиозакладок. Например, если при обнаружении жучка приблизить детектор к нему на небольшое расстояние, то приборы с маленьким динамическим диапазоном никак на это не отреагируют, т. к. они чувствуют разницы. А детекторы с гораздо более широким динамическим диапазоном (такие как

BugHunter-2 и BugHunter-1) покажут, что сигнал от жучка стал сильнее, т. е. вы двигаетесь в верном направлении и быстро определите место, где была заложена шпионская закладка.

Обновленный дизайн. Инженеры изменили не только «начинку», но и поработали над внешним обликом детектора жучков BugHunter-2. В результате новая модель стала еще более стильной, удобной и простой в использовании, чем ее предыдущая модель. По остальным же параметрам новый детектор BugHunter-2 полностью аналогичен своему предшественнику — популярному в странах СНГ антижучку BugHunter-1.

Рассмотрим **основные достоинства** антижучка BugHunter Профессионал BugHunter-2.

Он в точности соответствует всем указанным параметрам. Инженеры данного прибора гарантируют его высокое и надежную работу во всем заявленном диапазоне. Потрясающая надежность изделия была достигнута благодаря применению качественной, дорогой элементной базы европейского производства. Главная цель разработчиков создать точный, качественный детектор поля, не имеющий аналогов на рынке средств защиты информации — и им это действительно удалось!

Обладает полным частотным диапазоном. Данный прибор, охватывает весь диапазон, в котором работают жучки прослушки, от 50 до 3000 МГц, и имеет равномерную чувствительность на всех частотах этого диапазона. Индикатор поля BugHunter-2 имеет внутреннюю и внешнюю антенну (для низких частот) и высококачественную элементную базу, что позволяет ему одинаково хорошо работать на всем частотном диапазоне.

Современная электронная начинка позволила также реализовать сверхвысокий уровень чувствительности — 50 мВ/м!

Это интересно знать.

Абсолютное большинство антижучков, которые представленные на рынке, имеют чувствительность 100 мВ/м. это означает, что сигнал жучка они могут обнаружить только, когда его мощность превышает уровень в 100 мВ/м. Проще говоря, чувствительность этих приборов и дальность обнаружения в 2 раза ниже, чем у BugHunter-2.

Обнаружение короткоимпульсных (цифровых) жучков. Высокоскоростная элементная база детектора жучков BugHunter-2 позволяет

засечь даже цифровые жучки, которые передают информацию очень короткими импульсами, а затем на время «замолкают».

BugHunter-2 разработан специалистами оборонного предприятия. Все комплектующие прибора европейского производства изготовлены на заводах мировых лидеров в области радиоэлектроники. Каждая деталь имеет высочайшее качество, что гарантирует надежность прибора.

BugHunter Бизнес — детектор жучков и скрытых видеокамер

Рис. 4.4. Внешний вид BugHunter Бизнес

BugHunter Бизнес (**рис. 4.4**) — современный, компактный, легкий в использовании универсальный детектор жучков и беспроводных камер. Прибор необходим прежде всего бизнесменам и людям, часто ведущим конфиденциальные встречи и переговоры. BugHunter Бизнес предназначен для мгновенной оценки ситуации и принятия решения: продолжать переговоры или перенести на другое время, в другое место.

Прибор стилизован под зажигалку, он не привлечет внимания окружающих.

Оснащен двумя видами индикации:

- световой (светодиод на лицевой панели);
- звуковой (по звуку напоминает звук пришедшей sms).

Благодаря BugHunter Бизнес можно быстро и эффективно оценить ситуацию в месте встречи. Для этого необходимо включить прибор в режим монитора. Можно держать прибор в руках или положить в карман. При обнаружении беспроводной камеры или подслушивающего устройства начинает мигать светодиод дисплея и срабатывает звуковой сигнал, значит в месте встречи идет съем и передача информации.

Автоматически настраиваемая чувствительность позволяет проводить сканирование на различных расстояниях и разных каналах. BugHunter Бизнес улавливает радиоволны с частотой от 50 МГц до 3 ГГц, обнаруживая тем самым практически все беспроводные камеры и подслушивающие устройства. Используемое в устройстве специальное техническое и схемное решение устраняет помехи и значительно уменьшает число ложных срабатываний.

Детектор обладает всеми достоинствами профессионального оборудования, при этом может легко использоваться в повседневной жизни.

Технические характеристики:

- рабочий диапазон.....от 50 МГц до 3 ГГц;
- стилизован ..... под зажигалку;
- предназначение: для мгновенной оценки ситуации и принятия решения: продолжать переговоры или перенести на другое время, в другое место;
- питание ..... батареи cr2032, 2 шт.;
- размер, мм.....138×75×22;
- вес, г .....28.

BugHunter Базовый — детектор жучков и скрытых видеокамер

BugHunter Базовый (**рис. 4.5**) — это современный, компактный, легкий в использовании универсальный детектор жучков и беспроводных камер. Используется для обнаружения подслушивающих устройств и скрытых видеокамер. Прибор предназначен для широкого круга пользователей. Он прост и надежен в эксплуатации. Прибор стилизован под брелок. Его сложно всегда носить его с собой.

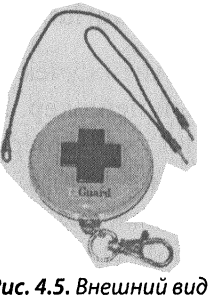


***Рис. 4.5.** Внешний вид BugHunter Базовый*

Технические характеристики:

- предназначение: для широкого круга пользователей;
- рабочий диапазон.....от 10 МГц до 3 ГГц;
- стилизован .....под брелок;
- размер, мм..... диаметр 60 мм, толщина 15;
- питание .....2 × cr2032;
- вес, г .....60.

Производитель: Тайвань.

BugHunter Black — детектор жучков и скрытых видеокамер

Детектор жучков «BugHunter Black» (**рис. 4.6**) — высокотехнологичный детектор для обнаружения и поиска любых радиопередающих устройств (жучков, скрытых камер, раций, сотовых и радиотелефонов). Его размер равен размеру обычной кредитной карточки! Позволяет искать не только аналоговые, но и цифровые подслушивающие устройства.

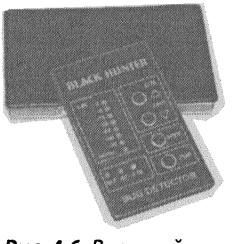


***Рис. 4.6.** Внешний вид BugHunter Black*

Технические характеристики:

- диапазон рабочих частот, МГц .....50—3000;
- чувствительность, мВ/м, не менее 100;
- динамический диапазон, дБ, не менее.....40;
- режимы работы..... сторожевой, поиск, акустозавязка;
- дальность обнаружения (в условиях спокойного радиоэфира, если нет рядом каких-либо передающих антенн и ретрансляторов) радиопередатчика 5 мВт, м, не менее.....5;
- дальность обнаружения сотового телефона, м, не менее.....20;
- габариты, мм ..... 77 × 47 × 5.

BugHunter Apollo — детектор жучков и скрытых видеокамер

Антижучек BugHunter Базовый (**рис. 4.7**) закамуфлирован под обычный **пейджер**. Профессиональная система обнаружения радиоизлучения любых передающих устройств и шпионской техники: подслушивающих устройств, радиожучков, сотовых телефонов стандартов GSM, DAMPS, AMPS, DECT и переносных радиостанций.

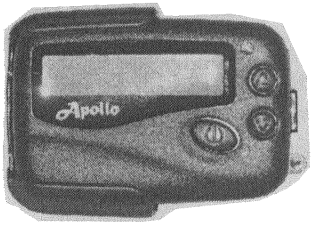


Рис. 4.7. *Внешний вид BugHunter Apollo*

Отличительной особенностью модели является то, что прибор имеет **частотомер**. Это позволяет не только осуществлять поиск жучков по уровню излучения (принцип горячо-холодно), но и видеть ЧАСТОТУ излучателя. Это позволяет быстрее найти и обнаружить жучек. Производство: Россия.

Технические характеристики:

- диапазон рабочих частот, МГц .....100—2800;
- чувствительность, мВ/м, не менее 100;
- динамический диапазон, дБ, не менее.....44;
- режимы работы: сторожевой, поиск, частотомер;
- дальность обнаружения радиопередатчика 5 мВт, м, не менее... 5;
- дальность обнаружения сотового телефона (мощности 100 мВт), м, не менее 20;
- габариты, мм ..... 60 × 40 × 18;
- длительность непрерывной работы от одной пальчиковой батареи LR03 (AAA), ч, не менее 24;
- варианты индикации при обнаружении жучка: цифровой ЖК-дисплей, светодиод, звук, вибро.

BugHunter SP77 — детектор жучков и скрытых видеокамер

BugHunter SP77 (**рис. 4.8**) — идеальное устройство для профессионалов. Предназначен для оперативного обнаружения и поиска радиоизлучающих устройств, в том числе:

- радиомикрофонов;
- телефонных радиоретрансляторов;
- радиостетоскопов;
- скрытых видеокамер с передачей информации по радиоканалу;
- радиомаяков систем слежения за перемещением объектов;
- несанкционированно включенных радиостанций и радиотелефонов.

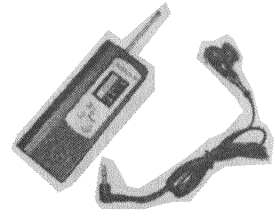


Рис. 4.8. *Внешний вид BugHunter SP77*

Этот прибор по функциональности подобен BugHunter Black, но, в отличие от него, имеет более высокое качество обнаружения за счет наличия внешней антенны. Его более низкая стоимость объясняется отсутствием стилизации корпуса — камуфляжа (BugHunter Black стилизован под кредитную карту).

Режимы работы: поиск, акустозавязка, сторожевой.

Индикация: звуковая, световая.

Функциональные особенности:

- десятисегментная светодиодная шкала;
- наличие выхода на наушники;
- наличие телескопической антенны улучшает качество обнаружения;
- возможность отключения звуковой индикации;
- возможность отключения режима акустозавязки.

Технические характеристики:

- диапазон рабочих частот, МГц .....50—3000 (весь диапазон, на котором работают жучки и скрытые камеры);
- чувствительность, мВ/м, не менее ..... 100 (высокая чувствительность);
- динамический диапазон, дБ, не менее..... 40;
- дальность обнаружения в условиях спокойного радиоэфира (если нет рядом каких-либо передающих антенн и ретрансляторов):
  - радиопередатчика 5 мВт, м, не менее.....5;
  - сотового телефона, м, не менее.....20;
- габариты, мм ..... 102 × 64 × 20.

BugHunter DVideo — обнаружитель скрытых видеокамер

BugHunter DVideo (**рис. 4.9**) — это шанс раз и навсегда избавиться от подглядывания. Детектор обнаруживает не радиоизлучение от работающей камеры, а фиксирует световые блики, отраженные от линз, которыми оснащены все объективы. Это позволяет прибору выявлять ЛЮБЫЕ скрытые и замаскированные видеокамеры (как проводные, так и беспроводные), даже неработающие в данный момент.

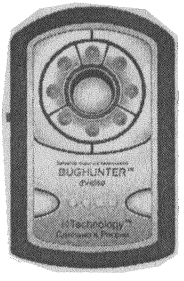


Рис. 4.9. Внешний вид BugHunter DVideo

BugHunter DVideo поможет отыскать и обезвредить все камеры, спрятанные в одежде, сумках, различных упаковках, потолках, стенах, внутри электромагнитного экрана и т. д. При своей компактности и небольшой мощности обнаружитель эффективно выявляет скрытые камеры на расстоянии до 10 м.

BugHunter Dvideo обладает самой доступной ценой на приборы подобного класса в России! Производитель: Тайвань.

Технические характеристики:

- расстояние эффективного обнаружения, м.....8—10;
- обнаруживаемая оптика..... PINHOLE, CMOS, CCD;
- питание..... аккумуляторные батареи LI-ON;
- время работы от батареи, ч..... 2,5—3;
- количество режимов отображения объекта..... 5;
- температура окружающей среды при зарядке, °С.....+10...+45;
- рабочий диапазон температур, °С.....–10...+55;
- температура при хранении, °С.....–20...+55;
- размеры, мм.....60×45×14;
- вес, г..... 70.

DT1 — универсальный детектор жучков и скрытых камер

Универсальный детектор камер и детектор жучков, детектор прослушки DT1 (**рис. 4.10**) — очень компактный детектор, выполняющее все функции поиска жучков и камер. Детектор обнаруживает все радиопередающие и скрытые устройства для съема информации, а также обнаруживает все линзы скрытых проводных и даже беспроводных мини камер.

Очень простая конструкция и возможности детектора камер + детектора жучков, детектора прослушки DT1 делают его очень легким в использовании.

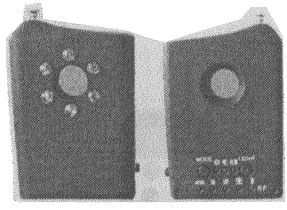


Рис. 4.10. Внешний вид детектора жучков и скрытых камер DT1

С частотным диапазоном от 1 МГц до 6,5 ГГц, детектор камер + детектор жучков, детектор прослушки DT1 способен обнаружить:

- все типы радиозакладок и устройств съема информации;
- приборы для слежения за авто (трекеры и маячки).

При обнаруженном сигнале жучка или прослушки, универсальный детектор камер + детектор жучков, детектор прослушки DT1 оповещает пользователя светодиодным индикатором на панели и звуковым сигналом с вибрацией.

Найти место точной закладки жучка можно с помощью светодиодных индикаторов, по изменению звукового сигнала и вибрации универсального детектора камер, детектора жучков, детектора прослушки DT1.

Детектор камер и жучков в одном предназначен и для эффективного и точного обнаружения любых (проводных и беспроводных) скрытых мини видеокамер (включенных и даже выключенных). Данный прибор оснащен специальным глазком и светодиодами.

Осматривая помещение через инфракрасный фильтр детектора (глазок), пользователь сможет с легкостью обнаружить скрытую видеокамеру благодаря блику от ее объектива, который в окне детектора будет выглядеть бликом желтого цвета на фоне затемненных красным фильтром других предметов.

Характеристики лазерного детектора линз и миникамер:

- рабочий частотный диапазон ..... от 1 МГц до 6,5 ГГц;
- дальность эффективного обнаружения ..... от 50 см до 5 м.

Характеристики индикатора обнаружения РЧ-сигнала:

- звуковой сигнал при обнаружении сигнала ..... есть;
- вибрация при обнаружении сигнала..... есть;
- регулировка чувствительности для точного обнаружения . есть;
- длина волны для обнаружения, нм 920;
- питание от встроенной батареи, ч 8;
- размеры, мм ..... 65×48×14.

ВН-02 — брелок-детектор жучков и беспроводных камер

Рис. 4.11. Внешний вид брелока-детектора жучков и беспроводных камер ВН-02

Детектор (индикатор) поля для обнаружения беспроводных радио видеокамер и беспроводных жучков ВН-02 (**рис. 4.11**) способен быстро обнаружить, есть ли в помещении беспроводная камера или беспроводный жучек.

Благодаря широкому диапазону улавливаемых частот от 100 МГц до 3000 МГц — данный детектор обнаружит любые активные беспроводные камеры или жучки. Он имеет 2 уровня чувствительности, благодаря которым можно не только узнать, есть ли в помещении беспроводная видеокамера, но и с помощью более чувствительного уровня детекции можно локализовать ее местонахождение. Так же благодаря своим небольшим размерам — он может использоваться в виде брелока.

Характеристики:

- дальность обнаружения радиоизлучения от беспроводных камер и жучков, м ..... до 10;
- количество уровней чувствительности для общего и более точного поиска беспроводных камер и жучков 2;
- звуковая и световая индикация найденных радио сигналов ..... есть;
- возможность ношения в виде брелока ..... есть;
- выдвигаемая металлическая антенна ..... есть;
- детектируемый диапазон частот, МГц ..... 100—3000;
- питание ..... батарейка 23А;
- размеры, мм ..... 68 × 35 × 14;
- вес, г ..... 26.

СОВА-V — индикатор поля для термо-радиочастотного поиска жучков

Назначение. Портативный поисковый прибор «СОВА-V» предназначен для поиска «радиожучков» по радиоизлучению (**Режим F**) и по тепловому излучению (**Режим С**). Внешний вид прибора представлен на **рис. 4.12.**

Рис. 4.12. Внешний вид прибора «СОВА-V»

В **режиме F** прибор позволяет обнаружить радиоизлучающие «жучки» любой мощности, диапазоном от 16 МГц до 6,5 ГГц.

В **режиме C** прибор позволяет обнаружить «жучки» с сетевым питанием и передачей информации через проводные каналы утечки информации.

Переключение между режимами поиска (C/F) осуществляется путем нажатия на кнопку, которая находится над батарейным отсеком.

Технические характеристики:

- минимально фиксируемая разность температур, °С..... 0,1;
- дальность измерения температуры, м.....до 1,5;
- диапазон частот детектора поля, МГц.....16—6500;
- время работы прибора (зависит от емкости батареи), ч ....3—6;
- примерная цена, долларов .....500.

Принцип работы в режиме F «Поиск по радиоизлучению». В этом режиме прибор производит поиск радиожучков методом определения источников излучения в помещении.

Для поиска радиожучков необходимо:

- переключить прибор в режим F (на экране прибора загорится значок «F», лазерный указатель отключится);
- отключить все излучающие устройства в зоне поиска: базовые станции телефонов DECT, радиопередающие интернет-модемы, радиопередающие сетевые роутеры и пр.
- проверить все подозрительные предметы, а также возможные места для закладки «радиожучков» в помещении.

Это интересно знать.

Если при приближении к какому-либо предмету уровень поля повышается, то в нем вероятно установлен «радиожучек».

К **подозрительным предметам** можно отнести:

- авторучки;
- калькуляторы;
- комнатные растения;
- сувениры;
- телефоны и факсы;
- кондиционеры;
- светильники;
- телевизоры;
- компьютеры.

К «полезным» излучающим устройствам можно отнести мобильный телефон и DECT радиотелефон.

Уровень излучения «радиожучков» может быть от малого до сверхмощного, поэтому дальность обнаружения для разных видов может отличаться.

Принцип работы в режиме С «Поиск по тепловому излучению». В этом режиме происходит поиск «жучков» методом поиска теплоизлучения производимого работой радиоэлектронных устройств питающихся от сети или телефонной линии.

Для поиска «жучков» необходимо:

- переключить прибор в режим С (на экране прибора загорится значок «С», лазерный указатель включится);
- навести лазер на расстоянии до 1,5 м рядом с подозрительным предметом и замерять уровень теплового излучения;
- навести на подозрительный предмет.

Это интересно знать.

Если уровень повысился: предмет излучает в тепловом диапазоне, возможно в нем установлен «жучек».

К **подозрительным предметам** можно отнести:

- розетки;
- удлинители;
- противопожарные датчики;
- выключатели питания;
- коробки развода сетей;
- коробки телефонной разводки;
- датчики сигнализации.

Рассмотрю некоторые **особенности использования** прибора в режиме поиска С. Если удлинители и розетки 220 В излучают в тепловом диапазоне, возможно, это вызвано искрением контактов. Из розеток необходимо выключить, по возможности, все устройства.

При измерении нужно убедиться в том, что рядом нет предметов, которые могут повлиять на результаты измерения: батарей отопления, осветительных приборов и пр.

Скрытая видеокамера добавляет примерно 5—12 °С, а обычный «радиожучок» 2—4 °С.

Будьте осторожны.
*Если на экране прибора загорелся значок «**Батарея**», значит, батарея прибора разряжена. Прибор может не правильно определять наличие радиоизлучения или теплоизлучения. Батарею необходимо заменить.*

Talisman — индикатор поля в диапазоне 3,5— 9800 МГц, созданный в виде зажигалки

Назначение. Индикатор поля предназначен для обнаружения «радиожучков» в офисах и автомобилях.

Технические характеристики:

- диапазон рабочих частот, МГц ..... 3,5—9800;
- регулировка уровня чувствительности индикатора, дБ..... 16;
- напряжение питания Li-pol, В..... 3,8;
- время заряда аккумулятора, ч..... 3.

Внешний вид прибора представлен на **рис. 4.13**.

Варианты использования индикатора.

Вариант 1. Поиск «радиожучков» в офисе и салоне автомобиля. Поиск «радиожучков» производится путем приближения индикатора к месту контроля. В офисе обязательно проверяются авторучки, калькуляторы, телефоны, сувениры и тумбочки стола. В машине проверяются сиденья, бардачок и багажник. При приближении к «радиожучку» светодиодный индикатор загорится желтым, а затем красным цветом.

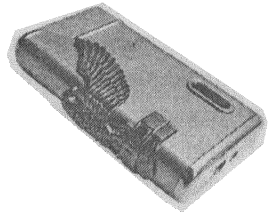


Рис. 4.13. Внешний вид прибора «Talisman»

Вариант 2. Обнаружение факта передачи информации посетителем с помощью мобильного телефона или передающей видеокамеры. Во время беседы индикатор «Зажигалка» устанавливается на столе таким образом, чтобы светодиодный индикатор был виден только хозяину помещения.

Если при заходе посетителя светодиодный индикатор **перейдет в «желтый» и далее в «красный» режим**, то это свидетельствует о том, что у посетителя работает передающее устройство. Это может быть радиостанция, передающая видеокамера, или мобильный телефон. Причем мобильный телефон может быть активирован не только посетителем, но и другими людьми.

Если во время беседы с посетителем индикатор **перейдет в «красный» режим** и при этом не будет звонка мобильного телефона посетителя или хозяина помещения, то это может свидетельствовать о несанкционированном использовании телефона в качестве «радиожучка». Для подтверждения этой версии надо молча (без комментариев) отстегнуть аккумулятор от мобильного телефона. При этом индикатор должен вернуться в «зеленый» режим.

Это интересно знать.
Систематическое срабатывание индикатора во время совещаний может свидетельствовать о заложенном в помещении «радиожучке» с дистанционным управлением.

Вариант 3. Обнаружение «радиомаяков», определяющих местоположение вашего автомобиля. За индикатором в салоне автомобиля должен наблюдать пассажир. Большинство «радиомаяков» осуществляют передачу данных по GSM каналу через фиксированные интервалы времени: от двух до тридцати минут. Когда нет звонков мобильных телефонов, и сработал индикатор, необходимо записать время срабатывания. Если интервалы времени между срабатываниями будут повторяться, то необходимо произвести поиск «радиомаяка».

Включение, регулировка и зарядка аккумулятора. Включение индикатора осуществляется путем нажатия на отсек, отвечающий за воспламенение зажигалки. Для выключения надо повторно нажать на данный отсек.

Регулировка чувствительности осуществляется подстроечным резистором, находящимся в нише «факела». При повороте этого резистора вправо чувствительность индикатора возрастает. Однако при этом и растет восприимчивость индикатора к внешним полям, и он все время начинает работать в «красном» режиме. В этом случае необходимо уменьшить чувствительность, повернув ручку немного влево.

Зарядное устройство вставляется в нижний отсек зажигалки (вместо заправки газом). Зарядка осуществляется до тех пор, пока индикаторная лампа на зарядном устройстве не погаснет.

Каракурт — прибор для обнаружения и пресечения работы жучков с ДУ

Назначение. Прибор предназначен для обнаружения и пресечения работы «жучков» с дистанционным управлением, работающих в диапазонах частот систем GSM, CDMA, DCS, 3G.

Будьте осторожны.
Запрещается использование прибора вне пределов своего помещения.

Технические характеристики:

- диапазоны частот выявляемых «жучков» с ДУ, МГц....824—849, 890—915, 1710—1785, 1920—1990;
- напряжение питания, В.....4,8
- емкость NiMh аккумулятора, мА/ч.....1800;
- ток заряда, мА.....90;
- дальность обнаружения 3G, CDMA, м..... до 4;
- Дальность обнаружения GSM, DCS, м.....5.

Внешний вид прибора представлен на **рис. 4.14**.

Конструктивное исполнение. На передней панели прибора размещены: тумблер включения питания, гнездо для зарядки аккумулятора, регулятор чувствительности приема и два светодиода индикации режимов.

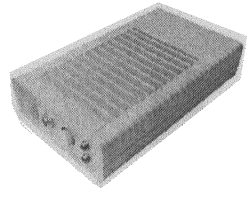


***Рис. 4.14.** Внешний вид прибора «Каракурт»*

Принцип действия. При включении питания, прибор в течение 16 с определяет приемники «жучков» с дистанционным управлением. В этом режиме красный светодиод мигает в течение 16 с. Далее прибор переходит в режим приема. Светодиод горит зеленым цветом.

Через 5—30 с GSM приемники «жучков» оживают и дают команду своим передатчикам на поиск базовой станции. Сигналы передатчиков «жучков» улавливаются приемником прибора MJ. Если обнаружен «жучек» GSM или DCS, то в течение 16 с мигает красный светодиод. При обнаружении «жучка» CDMA или 3G в течение 16 с мигает зеленый светодиод.

Для **локализации места положения «жучка»** необходимо уменьшить чувствительность индикатора, повернув ручку регулятора чувствительности влево. Снова включить питание и засечь факт активизации передатчика «жучка» в меньшей зоне помещения.

Если прибор используется во время совещания, а участники переговоров не успели отреагировать на сигнал индикатора, то утечки информации в помещении не произойдет. Приемник прибора вычисляет частоту излучения радиожучка CDMA GSM, DCS или 3G, ставит на частоте его приема точную помеху и заставляет его непрерывно перестраиваться.

Прибор не создает помех другим средствам связи вне заданного помещения, так как его радиус действия определяется чувствительностью приемника и не превышает 4—5 м.

Зарядка аккумулятора. Зарядка аккумулятора производится специальным зарядным устройством в течение 18—20 ч. Перед работой устройство необходимо зарядить.

Guard-MS — Bluetooth мобильный скремблер для защиты телефонов от прослушки

Назначение. Мобильный скремблер обеспечивает закрытие канала мобильной связи. Мобильный скремблер не позволяет системам радиомониторинга мобильной связи осуществлять «прослушку» по ключевым словам и характерным изменениям интонации голоса.

Будьте осторожны.
У абонента на другой стороне должен быть аналогичный прибор.

Технические характеристики:

- максимальная дальность связи между блоком MS и телефоном, м ..... до 3;
- минимальное расстояние между блоком MS и мобильным телефоном, м ..... от 0,5;
- максимальное время заряда LI-ION аккумулятора, ч..... до 10;
- время работы блока MS с полностью заряженным аккумулятором, ч..... до 8.

Рис. 4.15. Внешний вид прибора «Guard-MS»

Внешний вид прибора представлен на **рис. 4.15.**

Подготовка к работе. Перед началом работы скремблер необходимо зарядить. Включить скремблер. Регистрировать скремблер на своем телефоне (регистрируется, как обычная гарнитура Bluetooth).

Это интересно знать.
Регистрацию необходимо проводить только один раз, в дальнейшем при включении устройства Guard-MS, автоматически будет подключаться к вашему телефону.

Регистрация на разных моделях телефонов отличается, но принцип регистрации схож: Bluetooth → Создать подключение → Выбрать устройство«Guard-MS»

Работа с устройством Guard-MS. В телефонном разговоре договориться об использовании Guard-MS. Позвонить абоненту. Обоим абонентам включить устройства Guard-MS (предварительно зарегистрированных на телефоны).

Подождать 8 с пока устройства Guard-MS подключатся к телефонам (появляется значок гарнитуры на телефоне). Теперь можно вести разговор через устройства Guard-MS.

Если есть необходимость в использовании закрытого канала - боковым тумблером переходим в СИНИЙ режим. Если нет необходимость в использовании закрытого канала - боковым тумблером переходим в ЗЕЛЕНЫЙ режим. Оптимальная громкость для работы выбирается на телефоне и зависит от его модели.

МАЯК — камуфлированный индикатор поля под часы

Назначение. Индикация подслушивания разговора из помещения через средства мобильной связи посетителей; индикация несанкционированной активации своего мобильного телефона для подслушивания разговоров, в помещении; индикация радиооблучения мощным источником СВЧ радиосигнала, вредного для здоровья персонала помещения.

Технические характеристики:

- диапазон контролируемых частот, МГц ..... 160—65000;
- количество градации уровня чувствительности 3;
- средний ток потребления индикатора поля, мА 32;
- напряжение питания..... 220 В, 50 Гц.

Внешний вид прибора представлен на **рис. 4.16.**

Рис. 4.16. Внешний вид прибора «МАЯК»

Принцип действия. Если хозяин помещения или кто-либо из посетителей при-

нимает вызов по мобильному телефону, то индикатор уровня радиополя показывает наличие излучений в помещении. Такое повышение уровня является безопасным, так как получение или передача звонка наблюдается на мобильном телефоне.

Если звонок отсутствует, а при этом система индикации показывает повышение уровня радиополя, то это значит, что мобильный телефон дистанционно активирован на передачу и работает как «жучок». Такая работа должна быть длительной (несколько минут). На кратковременные повышения уровня индикатора обращать внимание не следует, так как это могут быть технические переключения телефонов между базами.

Это интересно знать.
При наличии в кабинете мощного «жучка» с дистанционным управлением повышение уровня индикатора будет происходить при его включении на передачу.

Если в помещении используется радиотелефон стандарта DECT или радиомодели, то уберите их на расстояние не менее 3 м, так как они непрерывно излучают СВЧ колебания.

В качестве индикатора уровня радиополя используется двухцифровой индикатор. После включения питания уровень текущего поля (от 00 до 99) будет высвечиваться на индикаторе. При включении мобильного телефона или «радиожучка» он будет повышаться.

Совет.
В местах, где большой первоначальный уровень радиополя его можно уменьшить, нажав на специальную кнопку на задней панели часов.

Всего прибор имеет три градации чувствительности. При нажатии кнопки значение 11 соответствует максимальной чувствительности (по умолчанию); 22 — средняя чувствительность; 33 — слабая чувствительность (для работы в условиях сильных помех).

Ратник — стационарный прибор для обнаружения жучков с ДУ

Назначение. Прибор предназначен для обнаружения работы «жучков» с дистанционным управлением, работающих в диапазонах частот систем GSM, CDMA, DCS, 3G.

Технические характеристики:

- диапазон рабочих частот передающей части, МГц ..... 865—895, 935—960, 1805—1890, 2110—2180.
- радиус создания помех, м.....4—6;
- параметры электропитания..... 220 В, 50 Гц;
- диапазон рабочих температур, °С .....от -10 до +30.

Будьте осторожны.
Запрещается использование прибора вне пределов своего помещения.

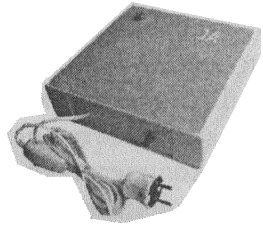


Рис. 4.17. Внешний вид прибора «Ратник»

Внешний вид прибора представлен на **рис. 4.17.**

Принцип действия. При первоначальном включении питания, прибор в течение 16 с определяет приемники «жучков» с дистанционным управлением. При этом индикатор на передней панели мигает красным светом в течение 16 с.

Далее прибор переходит в **режим приема.** В этом режиме индикатор горит зеленым светом.

Через 5—30 с приемники «жучков» оживают и дают команду своим передатчикам на поиск базовой станции. Сигналы передатчиков «жучков» улавливаются приемником прибора. Снова производится блокировка приемника «жучка» на 16 с. Если обнаружен «жучек» GSM или DCS, то индикатор мигает красным светом. При обнаружении «жучка» CDMA индикатор мигает зеленым.

Для локализации места положения «жучка» необходимо разделить помещение на условные части и уменьшить чувствительность индикатора, повернув ручку регулятора чувствительности влево. Снова включить питание и засечь факт активизации передатчика «жучка» в данной части помещения.

Если прибор используется во время совещания, а участники переговоров не успели отреагировать на сигнал индикатора, то утечки информации в помещении не произойдет. Приемник прибора вычисляет частоту излучения радиожучка CDMA GSM, DCS или 3G, ставит на частоте его приема точную помеху и заставляет его непрерывно перестраиваться.

Прибор не создает помех другим средствам связи вне заданного помещения, так как его радиус действия определяется чувствительностью приемника и не превышает 4—5 м.

Сапфир — устройство для скрытого обнаружения диктофонов и видеокамер

Назначение. «Сапфир» позволяет скрытно обнаружить использование видеокамеры, видеодиктофона или диктофона. Перечисленные изделия могут быть расположены на теле человека, установлены в автомобиле или замаскированы в различные аксессуары: папки, барсетки, часы, пульты автомобильной сигнализации и т. д. Возможно использование «Сапфира» для поиска диктофонов и специальных видеокамер, в том числе с антибликовым покрытием.

Технические характеристики:

- количество основных частот магнитных полей 200;
- количество подчастот каждой основной частоты 10;
- дальность обнаружения проводных видеокамер, см ..... до 40;
- дальность обнаружения видеокамер с записью на флеш-память, см ..... до 50;
- дальность обнаружения записи на диктофон, см ..... до 90;
- емкость аккумулятора Li-ion 3,7 В, мА/ч 2400;
- время непрерывной работы, ч.....12;
- время заряда аккумулятора, ч.....9.

Внешний вид прибора представлен на **рис. 4.18.**

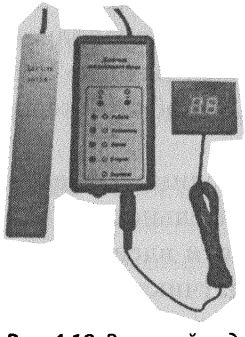


Рис. 4.18. Внешний вид прибора «Сапфир»

Принцип действия прибора основан на выявлении очень слабых магнитных полей, создаваемых видеокамерой или диктофоном. В память устройства занесены частоты полей большинства видеокамер и диктофонов, используемых для скрытой видеозаписи. При появлении новых устройств имеется возможность занести их параметры излучения в память изделия для их дальнейшего обнаружения.

Состав изделия: основной блок с выносным датчиком поля; индикатор уровня магнитного поля; шнур для зарядки; сумка для переноски.

Назначение органов управления. В верхней части основного блока имеется включатель питания и гнездо для подключения индикатора уровня или шнура зарядного устройства. На передней панели расположены кнопки различного функционального назначения. При включении питания или нажатии кнопки «Работа» прибор переходит в основной функциональный режим. Кнопкой «Установка» прибор переводится в режим записи параметров излучения новых изделий.

Запись и стирание параметров магнитного поля новых изделий производится кнопкой «Запись» и «Стирание».

Кнопки «+» и «–» в режиме «Работа» изменяют чувствительность устройства, а в режиме «Установка» — частоту настройки изделия.

При достижении пределов регулировки «+» и «–» напротив этих знаков постоянно горят соответствующие светодиоды.

Возле каждой кнопки загорается красный светодиод, индицирующий нажатие. Светодиод «Зарядка» горит во время заряда аккумулятора и гаснет при его полном заряде.

В режиме «Работа» прибор поочередно перебирает все ранее записанные сигналы полей и сравнивает с сигналами, поступающими с выносного датчика поля. Индикатор уровня магнитного поля показывает изменение магнитного поля, при приближении датчика к видеокамере или диктофону.

Режим обнаружения видеокамеры или диктофона на теле человека. Для работы в этом режиме основной блок устройства прячется во внутреннем кармане, а выносной датчик магнитного поля — в рукаве. Для крепления датчика поля на руке имеются специальные липучки системы петля-крючок. При включении питания прибор автоматически переходит в режим «Работа».

В этом режиме он сканирует все ранее запомненные параметры поля и сравнивает их с теми, которые поступают с датчика в рукаве. При их совпадении срабатывает вибро-мотор в блоке, расположенном во внутреннем кармане. Количество срабатывай 1—3 пропорционально уровню поля. Так как магнитные поля, создаваемые видеодиктофонами, очень слабые, то рука с датчиком поля должна пройти на расстояние 5—10 см от человека. При исследовании аксессуаров посетителей (папок, барсеток, часов и т. д.) датчик должен находиться от них на расстоянии 5—10 см. Время обследования каждой точки не должно быть меньше 0,3—0,4 с, так как за это время прибор перебирает 10—12 записанных частот.

Режим скрытного обнаружения видеокамеры или диктофона у посетителя в приемной. Выносной датчик магнитного поля устанавливается на разделительной стенке со стороны секретаря. Там же крепиться и индикатор уровня поля.

При приближении посетителя к секретарю, датчик магнитного поля улавливает излучение видеокамеры или диктофона. Секретарь по телефону докладывает начальнику об уровне «напичканности» посетителя.

Режим скрытого обнаружение видеокамеры или диктофона у посетителя за рабочим столом. Для работы в этом режиме выносной датчик магнитного поля устанавливается под столешницей приставного столика с помощью липучек. К основному блоку подключается индикатор уровня магнитного поля. Индикатор уровня магнитного поля устанавливается за рабочим столом таким образом, чтобы не был виден посетителю.

Если в барсетке, папке, часах, брелоке от машины посетителя замаскирована видеокамера или диктофон, то индикатор покажет увеличение уровня магнитного поля. Если камера установлена в галстуке, то увеличения уровня поля будет фиксироваться приближение галстука к краю стола.

Для максимальной чувствительности данной системы необходимо чтобы не было внешних магнитных полей от работающих видеокамер системы видеонаблюдения, от старых телевизоров, импульсных блоков питания и т. д.

Если в помещении имеется мешающее устройство, отключить которое невозможно, то необходимо перейти в режим «Установка», найти кнопками «+» и «–» частоту излучения этого устройства и нажатием кнопки «Стереть» удалить ее из списка.

Режим поиска работающих видеокамер и диктофонов. Современные видеокамеры все чаще используются с антибликовым покрытием, которое не позволяет их обнаруживать методом оптической локации. В этом случае их обнаружение возможно по магнитному полю работающей видеокамеры.

Для работы в этом режиме выносной датчик устанавливается на кронштейн или палку, а основной блок и индикатор магнитного поля находятся в руках. Выносным датчиком необходимо просканировать с интервалом 10—15 см все стены и потолки помещения. Если в каком-то месте происходит существенное изменение уровня, то это место необходимо более тщательно визуально осмотреть с помощью лупы и фонарика.

Это интересно знать.

Для поиска работающих диктофонов в интерьере помещения необходимо выключить компьютеры, зарядные устройства, блоки бесперебойного питания, факсы, принтеры и лампы с импульсными преобразователями напряжения.

Обследование диванов, столов, стульев, ниш проводиться с помощью датчика поля на минимально возможном расстоянии. Если сигнал, от какого либо электронного изделия зашкаливает и индикатор показывает число 99,то необходимо уменьшить уровень входного сигнала для точной локализации изделия. Уменьшение проводится кнопкой «–» в режиме «Работа».

Запись параметров излучения нового устройства. Исследуемое устройство включается в режиме видео или аудиозаписи и устанавливается в 3—4 см от датчика магнитного поля. На основном блоке нажимается и удерживается в течение 2 с кнопка «Установка». Индикацией переключения в режим установки служит красный светодиод напротив надписи.

Далее нажатием кнопки «+» изменяем частоту приема магнитного поля с датчика. Всего имеется 2000 различных частот приема. При ограничении максимальных показаний индикатора цифрами 99 отодвигаем исследуемое устройство от датчика магнитного поля и кнопками «+» и «–» снова добиваемся максимальных показаний.

Для более точной установки на частоту, необходимо еще раз нажать на кнопку «настройка». При этом светодиод напротив соответствующий надписи будет мигать. Кнопками «+» и «–» добиваемся максимальной подстройки. Если больших показаний добиться не удается, то нажимается кнопка «Запись», соответствующий светодиод двумя миганиями фиксирует в памяти параметры нового устройства.

Всего имеется 200 грубых частот и каждая из них имеет 10 точных подчастот.

Зарядка аккумулятора. Для заряда аккумулятора штекер зарядного кабеля необходимо подключить к основному блоку. Другой конец кабеля подключается к USB-разъему компьютера. При зарядке загорается светодиод индикации — «Зарядка». По окончании заряда он погаснет.

ГЛАВА 5

ПОДАВИТЕЛИ СОТОВЫХ ТЕЛЕФОНОВ И ДИКТОФОНОВ

Необходимо предупредить возможную утечку информации с помощью блокираторов информации, постановки активных помех устройствам сбора информации, которые могут быть поставлены в помещении или салоне автомобиля. Противошпионские штучки, созданные для информационной защиты, помогут избежать утечки важнейшей информации.

Блокираторы информации и глушилки

Блокираторы, или **глушилки**, работают по принципу радиопомех или акустических помех. **Блокираторы с помощью радиопомех** запрещены в странах СНГ, например, в Украине. Разумеется, они эффективны только в случае утечки информации по радиоканалам (на проводные жучки и диктофоны они не будут оказывать воздействия).

Акустические блокираторы информации — устройства, которые в момент переговоров создают блокаду акустической информации для диктофонов и жучков. Они, конечно же, слышны для переговорщиков, но зато идет полная защита информации по всем каналам.

Для чего нужна GSM глушилка сотовых телефонов

Сегодня непросто представить себе жизнь без сотовой связи. Надежная и быстрая телефонная связь почти с любой точкой мира, моментальная передача информации, работа в Интернете — в наши дни операторы связи предлагают нам огромное число сервисов. Однако одновременно с удобствами, пришедшими к нам с сотовыми телефонами, появилась и серьезная проблема информационной безопасности.

О том, что переговоры по телефону можно прослушать, знают все. А многие ли задумывались над тем, что мобильный телефон — это практически готовый «радиожучок», причем его можно прослушивать на расстоянии в тысячи километров!

При развитии микроэлектроники мобильные аппараты по своим характеристикам и размерам уже догнали специальные технические средства, и их обнаружить бывает очень непросто. В третьей главе отмечалось, что практически все мобильные телефоны имеют недекларированные возможности. Иными словами, даже отключенный, ваш мобильный телефон можно включить дистанционно на передачу.

Так что делать? Отказаться от такого незаменимого средства связи, как телефон? Не нужно, посмотрим, чем нам сможет помочь электроника.

Как мера борьбы с незаконным прослушиванием, были разработаны глушилки мобильных телефонов. Работа подобных приборов оказалась очень легкой. Все сотовые аппараты работают в диапазоне частот от 0,9 до 2,2 ГГц. Поэтому достаточно установить генератор шума (так называемая, **GSM глушилка**) в таком диапазоне, и телефон в радиусе действия подавителя работать не сможет.

В помещении, где работает глушилка телефонов, откажут все приборы, которые используют частоты из вышеуказанного диапазона. Например, всевозможные стационарные «прослушки» и передающие видеокамеры, которые сделаны на основе мобильных телефонов. Вернее, они смогут работать, но только их сигнал не пробьется через помеху подавителя.

В наше время есть масса подавителей сотовых телефонов, с различной мощностью и радиусами действия. Существуют переносные и стационарные модели. Переносная глушилка мобильных телефонов может выглядеть, как барсетка, кейс или пачка сигарет. Без подзарядки глушилка сотовых телефонов сможет работать от 10 мин. до нескольких часов. Этого вполне хватит, чтобы сделать доклад, провести беседу, совещание.

Исходя из вышесказанного, хотелось бы обратить внимание и на побочные эффекты устройств подавления. Если на встрече или совещании вы пользуетесь устройствами записи звука, скажем, цифровыми диктофонами, приготовьтесь к тому, что защита ваша может работать, как подавитель диктофонов, отмечается на www.zhuchkam.net.

BugHunter Кокон — подавитель акустического канала сотового телефона

Мобильный телефон — наш верный друг и помощник — оказывается может выполнять и функции шпиона. Мало кто знает о «полицейском режиме» телефонов GSM. В этом режиме мобильный

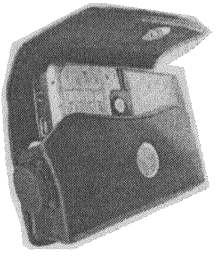


Рис. 5.1. Внешний вид BugHunter Кокон

телефон активируется дистанционно без внешних признаков входящего звонка (не загорается подсветка, нет сигнала вызова), и в радиусе нескольких метров от телефона любой разговор может быть подслушан.

Подавитель акустического канала БагХантер Кокон (**рис. 5.1**) обеспечивает защиту от прослушивания телефонных разговоров по мобильному телефону. Он улавливает такую активность телефона и создает сложное акустическое поле, которое превращает разговор собеседников в шум, что делает прослушивание бесполезным. Теперь вы можете не волноваться, что важная информация с деловых встреч, совещаний и важных переговоров станет доступна посторонним через канал сотовой связи вашего собственного телефона.

Прибор закамуфлирован под обычный чехол для мобильного — понять, что это такое на самом деле по внешнему виду невозможно.

Изделие имеет сертификат Гостехкомиссии России № 697. Используемая в изделии технология защищена патентом РФ № 2183914. Прибор произведен в России.

Принцип действия прибора. Принцип действия этого прибора прост, как и все гениальное: если столь непросто защититься от прослушивания, нужно сделать его бессмысленным. Действует этот прибор следующим образом: превращая речь собеседников в плавающие шумы, не только делает невозможным прослушивание ваших бесед, но и ставит под сомнение целесообразность периодической «проверки» ваших разговоров различной криминальной мелочью и мошенниками. Ведь результат все равно будет один: в записи появятся только нечленораздельные звуки, не подлежащие обработке ни одним фильтром, поскольку зашумление производится сложноструктурированным флуктуирующим акустическим полем.

Как работает. Трубка сотового телефона помещается во внутренний объем футляра. В случае негласной дистанционной активации телефона в режим прослушивания единственным признаком, по которому это можно обнаружить, является изменение напряженности электромагнитного поля (т. е. передатчик сотового телефона несанкционированно включается на передачу). Это изменение фиксируется индикатором поля, входящим в состав устройства, который дает команду на автоматическое включение акустического шумоге-

нератора, расположенного внутри прибора. Уровень акустического шума на входе микрофона трубки сотового телефона таков, что обеспечивается гарантированное закрытие этого канала утечки информации, т. е. зашумляется весь тракт передачи речевой информации таким образом, что на шпионском приемнике отсутствуют какие-либо признаки речи.

Внешний вид и дизайн. Данное устройство выполнено в виде стильного кожаного чехла, который удобно носить с собой. Он не привлечет никакого лишнего внимания со стороны окружающих и будет защищать вас абсолютно незаметно. Для монтажа устройства может быть использован практически любой чехол. При заказе изделия для оптимального размещения трубки в чехле необходимо указать модель телефона либо ее размеры. Устройство может быть установлено и в чехле, приобретенном самим клиентом с учетом габаритов защищаемого телефона (размер внутреннего объема чехла должен на 10 мм превышать длину телефонной трубки).

Технические характеристики:

- уровень шума в точке размещения микрофона сотового телефона, не менее, дБ 100;
- эффективный спектр шумового сигнала, Гц ..... 300—4000;
- питание ..... литиевая батарея типа CR2032;
- время непрерывной работы, не менее ..... 2 месяца.

BugHunter PS-1 — подавитель сотовых телефонов

Подавитель сотовых телефонов BugHunter PS-1 поможет обезопасить себя от угрозы подслушивания через мобильный телефон (даже в выключенном состоянии сотовый позволяет слушать разговоры на расстоянии нескольких метров) и подглядывания при использовании бепроводных видеокамер.

Кроме того, прибор позволит подавить любую активность сотовых телефонов в помещении, тем самым давая возможность спокойно и сосредоточенно провести совещание, доклад, спектакль, экзамен, защитить диссертацию и пр.

BugHunter PS-1 (**рис. 5.2**) подавляет сигналы, которые посылают шпионские камеры и мобильные телефоны, на расстоянии до 8—10 м.

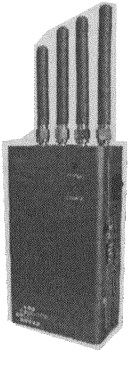


***Рис. 5.2.** Внешний вид BugHunter PS-1 1050*

Технические характеристики:

- расстояние эффективного подавления, м .....8—10;
- средняя выходная мощность каждой антенны, мВт 300;
- подавляемые частоты, МГц ... 845—975, 1785—2000, 100—2180;
- подавляемые стандарты.....AMPS, N-AMPS, NMT, TACS, GSM, CDMA, TDMA, IDEN, UMTS;
- питание, мА/ч .....литиевая батарея DC 12 В / 1600;
- время заряда батареи, ч.....2;
- время работы от батареи,ч..... 1,5—2;
- температура окружающей среды при заряде, °С ..... +10...+45;
- температура окружающей среды при работе, °С ..... –10...+55;
- температура окружающей среды при хранении, °С ... –20...+55;
- размер, мм..... 110 × 62 × 30;
- вес, г.....300.

Производитель: Тайвань

BugHunter Ладья — подавитель акустического канала сотового телефона

Рис. 5.3. Внешний вид BugHunter Ладья

Подавитель акустического канала BugHunter Ладья (**рис. 5.3**) обеспечивает защиту от прослушивания телефонных разговоров по мобильному телефону. Он улавливает такую активность телефона и создает сложное акустическое поле, которое превращает разговор собеседников в шум, что делает прослушивание бесполезным.

Теперь можно не волноваться, что важная информация с деловых встреч, совещаний и важных переговоров станет доступна посторонним через канал сотовой связи вашего собственного телефона.

Это интересно знать.

В отличие от модели BugHunter Кокон этот прибор выполнен в виде стильной карандашницы, которая отлично впишется в интерьер деловых кабинетов и офисов.

Изделие имеет сертификат Гостехкомиссии России № 698. Используемая в изделии технология защищена патентом РФ № 2183914. Производитель: Россия.

Технические характеристики:

- уровень шума в точке размещения микрофона сотового телефона не менее, дБ 100;
- эффективный спектр шумового сигнала, Гц .....300—4000;
- питание ..... две батареи типа ААА;
- время непрерывной работы от одного комплекта батарей, не менее .....6 месяцев.

В изделии реализован автоматический контроль разрядки батареи. Признаком разряда батарей является прерывистый тональный сигнал частотой 2 кГц с периодом повторения 0,6 с, слышимый на фоне шума.

Страна производитель: Россия.

GSM, CDMA Мозаика НЧ — блокировка мобильных телефонов

Мозаика НЧ (**рис. 5.4**) предназначена для защиты от прослушки помещений с использованием мобильных (сотовых) телефонов, а также жучков, которые используют сотовую связь, для передачи данных.

Рис. 5.4. Внешний вид Мозаика НЧ

Прибор выполнен в виде настольных часов-калькулятора, с полным сохранением их функций. **Отличительными особенностями серии «Мозаика»** являются:

- полное отсутствие влияния на любые другие радиоэлектронные устройства бытовой электронной техники (теле-, видео-, аудио- и др.), компьютеры, оргтехнику;
- блокировка одновременно любого количества каналов связи;
- возможность регулировки защищаемой площади в соответствии с границей выделенного помещения;
- прибор генерирует помехи приемным каналам телефонов, в результате они теряют связь с базовой станцией, и их нельзя использовать.

Функциональные особенности устройства:

- выполнен в виде настольных электронных часов с сохранением всех функций;
- подавляемые стандарты — GSM, AMPS, CDMA, DAMPS;
- может использоваться в автомобилях, на неподготовленных территориях и т. п. за счет автономного питания;
- не создает помех для других радиоэлектронных устройств;
- подавляет одновременно все каналы связи в радиусе действия 3—15 м.

Технические характеристики:

- стандарты подавления: GSM 900/1800, DAMPS, CDMA, AMPS, E-GSM;
- мощность, Вт 0,5;
- радиус действия, м .....3—15;
- антенна ..... внешняя скрытая (подставка под ручку);
- питание .....220 В/50 Гц.

BugHunter PD-1 — подавитель диктофонов

Современные цифровые диктофоны настолько малы и незаметны, что спрятать их где угодно не составляет труда. Чтобы защитить себя от угрозы записи информации при проведении важных переговоров, деловых встреч, совещаний, необходимо и достаточно использовать подавитель работы диктофонов BugHunter PD-1 (**рис. 5.5**).

Рис. 5.5. *Внешний вид BugHunter PD-1*

Прибор подавляет работу звуковых регистраторов, к которым относятся цифровые и кассетные диктофоны, на расстоянии до 8 м. BugHunter PD-1 компактен и работает абсолютно бесшумно, что позволяет использовать его открыто — не пряча от посторонних.

Кроме того, устройство подавления находится на передней панели прибора и закамуфлировано под часы, скрывая назначение прибора. В комплекте с подавителем поставляется пульт Д/У, выполненный в виде брелока, что упрощает управление прибором. Производитель: Тайвань.

Технические характеристики:

- расстояние эффективного подавления, м ..... до 8;
- средняя выходная мощность, Вт 3;
- вертикальный угол подавления, °..... 120;
- горизонтальный угол подавления, ° 150;
- питание ..... 100—240 В AC, 1,5 А;
- время заряда батареи, ч..... 4;
- время беспрерывной работы от батареи, ч 3;
- размер, мм..... 290 × 210 × 30;
- вес, кг..... 1,8.

Бриз — миниатюрный подавитель мобильных телефонов GSM

Рис. 5.6. Внешний вид подавителя мобильных телефонов GSM «Бриз»

Миниатюрный подавитель мобильных телефонов GSM «Бриз» (**рис. 5.6**) — небольшой блокиратор сотовых телефонов, который может использоваться на совещаниях, в конференц-залах, в режимных учреждениях и т. д. Эффективен против любых приборов видеонаблюдения, жучков прослушки, радиоуправляемых устройств и любых других, использующих для передачи данных каналы мобильной GSM связи. **Функциональные особенности блокиратора связи:**

- стандарты блокировки — GSM 900, GSM 1800/1900;
- небольшие размеры, малый вес, портативность;
- возможность работы от сети и в автономном режиме;
- индикация разряда батареи;
- высокая эффективность подавления.

Устройство представляет собой законченный блок, имеющий внешнее питание 9 В. Не имеет дополнительных антенн. Радиус действия прибора зависит от удаленности от станций сотовой связи. В среднем в городе радиус действия составляет 5—10 м. При использовании в непосредственной близости от станций радиус составит 1 м.

Технические характеристики:

- максимальный радиус действия, м 15;
- размеры, мм ..... 98 × 65 × 22;
- стандарты блокировки ..... GSM 900, GSM 1800/1900;
- мощность на выходе, Вт 0,76;
- мощность потребления, Вт 6;
- питание, Гц ..... 220 В, 50;
- время непрерывной работы ..... неограниченно;
- диапазон рабочих температур ..... от +5 до +40 °С;
- диаграмма направленности ..... круговая;
- антенны ..... внутренние.

MANGO-2 — генератор речеподобной помехи для защиты окон и подвесных потолков

Назначение. «MANGO-2» предназначен для защиты окон, подвесных потолков, ниш воздуховодов и междверных проемов от средств съема информации.

Технические характеристики:

- диапазон частот, Гц.....200—7500;
- минимальная нагрузка, Ом 4;
- мощность выходного сигнала, Вт.....2×6;
- электропитание, В .....220.

Внешний вид прибора представлен на **рис. 5.7**. Основная схема размещения излучателей речеподобного шума представлена на **рис. 5.8**.

Это интересно знать.
Признано, что генераторы речеподобной помехи эффективнее, чем генераторы белого шума.

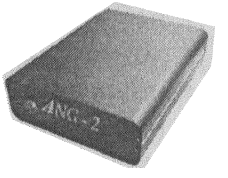


***Рис. 5.7.** Внешний вид прибора «MANGO-2»*

Принцип действия. Двухканальный генератор шума «MANGO-2» обеспечивает генерацию акустической речеподобной помехи в диапазоне частотного спектра от 200 Гц до 7,5 кГц.

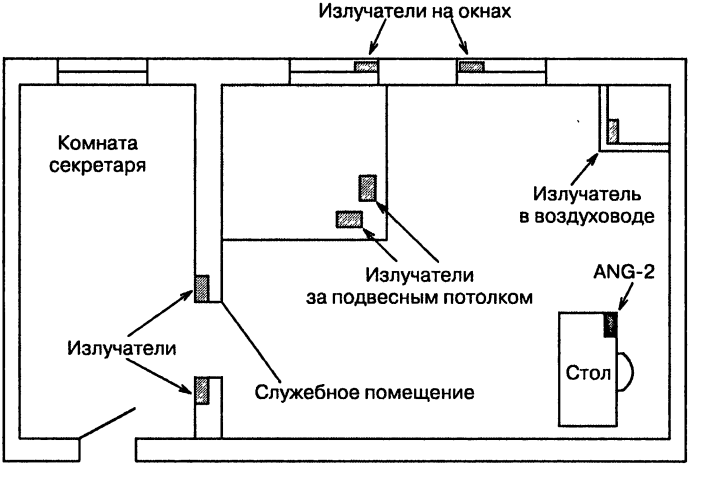


***Рис. 5.8.** Основная схема размещения излучателей речеподобного шума*

Мощность сигнала помехи на каждом из выходов может независимо регулироваться резисторами на задней стенке прибора. Изделие не создает помех устройствам бытовой электроники. Уровень акустического сигнала помехи практически не влияет на комфортность проведения переговоров.

Включение прибора. Сетевая вилка генератора шума включается в сеть 220 В. На передней панели включается тумблер. Загорание неоновой лампочки данного тумблера свидетельствует о включении прибора.

МПГ — мобильный подавитель диктофонов и жучков с индикатором поля

Назначение. Индикация прослушивания из помещения через средства мобильной связи или радиостанции. Поиск «радиожучков» в помещении или автомобиле. Защита от диктофонов при ведении переговоров с посетителем.

Технические характеристики:

- диапазон частот индикатора радиополя, ГГц .....0,12—6,2;
- максимальная мощность маскирующего сигнала, Вт..... 1,5;
- эффективный спектр маскирующего сигнала, Гц .....280—4300;
- емкость аккумулятора, мА/ч.....650;
- средний потребляемый ток, мА .....270.

Внешний вид прибора представлен на **рис. 5.9.**

Рис. 5.9. Внешний вид прибора «МПГ»

Использования прибора «МПГ» в режиме индикатора поля. При появлении вблизи стола посетителя с включенной на передачу радиостанцией или мобильным телефоном уровень индикатора поля существенно повысится по сравнению с фоновым значением.

Если хозяин помещения или кто-либо из посетителей принимает вызов по мобильному телефону, то цифровой индикатор уровня радиополя показывает наличие излучений в помещении.

Это интересно знать.

Такое повышение уровня над фоновым значением является безопасным, так как получение или передача звонка наблюдается на мобильном телефоне.

Если звонок отсутствует, а при этом резко повышается уровень, то это значит, что мобильный телефон дистанционно активирован на передачу и работает как «жучок». При этом надо иметь в виду, что такая работа должна быть длительной (несколько минут). На кратковременные повышения уровня индикатора обращать внимание не следует, так как это могут быть технические переключения телефонов между базами.

При наличии в кабинете мощного «жучка» или радиостанции с дистанционным управлением повышение уровня индикатора будет происходить при его включении на передачу.

Поиск «радиожучков» в помещение или автомобиле производится путем сравнения уровней излучения при приближении к подозрительному объекту.

Использование прибора «МПГ» для защиты от диктофона посетителя. Для ведения переговоров хозяин помещения предупреждает посетителя о важности темы и необходимости включения средства защиты. После включения питания прибор устанавливается динамиками в сторону посетителя и ближе к нему. Если в процессе переговоров необходимо сделать паузу, нужно нажать на регулятор громкости. Повторное нажатие приведет к возобновлению речеподобного маскирующего сигнала.

Использования прибора для акустической защиты помещения. Для акустической защиты помещения от диктофонов и «жучков», при ведении переговоров между партнерами необходимо подключить внешние акустические колонки. Они включаются в гнездо, обозначенное знаком наушников. Колонки направляются в разные стороны помещения. Их громкость устанавливается таким образом, чтобы аффективно маскировалась речь участников переговоров.

Зарядка аккумулятора. Зарядка аккумулятора производится через специальный USB-шнур, поставляемый в комплекте. Уровень заряда аккумулятора индицируется на дисплее. Для полного заряда он должен достигнуть 100%. Время заряда составляет 5—6 ч.

Гроза — стационарный акустический подавитель диктофонов

Назначение. Подавитель предназначен для предотвращения записи беседы на диктофон или ее передачи с помощью мобильного телефона посетителем из кабинета.

Технические характеристики:

- диапазон спектра маскирующего сигнала, Гц .....180—5400;
- мощность маскирующего сигнала, Вт ..... до 1,3;
- уровень подавления сигнала акустозавязки, дБ.....28;
- напряжение питания ..... 220 В, 50 Гц.

Внешний вид прибора представлен на **рис. 5.10.**

Состав. «Гроза» состоит из металлического блока, двух колонок и вынесенного микрофона с кнопкой включения динамиков прибора. Имеет дополнительный выход для установки акустических систем за подвесным потолком, мебелью и т. д.

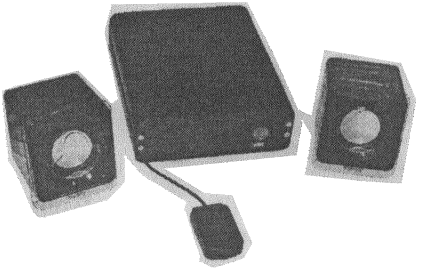


***Рис. 5.10.** Внешний вид прибора «Гроза»*

Принцип действия прибора. Маскирующий сигнал представляет собой речь хозяина помещения, преобразованную по случайному закону. Такое преобразование обеспечивает максимальный комфорт проведения переговоров и делает невозможным запись и очистку речи от помехи.

В ходе беседы хозяин кабинета акцентирует внимание собеседника на важности разговора и необходимости включения средства защиты, под тем предлогом, что в офисе может стоять «жучок». После этого он на одну секунду нажимает кнопку, установленную скрытно возле микрофона.

Для максимальной маскировки говорить необходимо в сторону микрофона.

Гюрза — автомобильный подавитель диктофонов АПД-7М

Назначение. Предотвращение записи беседы на диктофон в салоне автомобиля или в офисе.

Это интересно знать.

Акустические подавители диктофонов в настоящее время являются единственными эффективными средствами защиты от всех видов прослушивающих устройств.

Технические характеристики:

- время работы, ч..... 3,5—4;
- диапазон спектра маскирующего сигнала, Гц .....180—5400;

- уровень подавления сигнала акустозавязки, дБ.....:32;
- время зарядки аккумулятора, ч .....4—5;
- расстояние между АПД-7М «Гюрза» и приемником, м ..... до 6;
- емкость аккумулятора, мА/ч.....550.

Внешний вид прибора представлен на **рис. 5.11**.

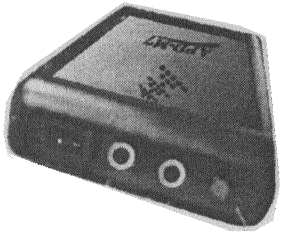


Рис. 5.11. Внешний вид прибора «Гюрза»

Конструктивное исполнение. АПД-7М «Гюрза» состоит из передающего блока, двух микрофонов, зарядного устройства и барсетки. АПД-7М «Гюрза» может использоваться для одновременной маскировки речи двух человек.

«Автомобильный» режим использования. Прибор настраивается на автомобильный приемник FM диапазона. Сам АПД-7М «Гюрза» может быть спрятан в кармане пиджака, а микрофон с кнопкой управления крепится под галстуком. Хозяин автомобиля говорит собеседнику о важности темы разговора, и необходимости включения средства защиты и нажимает кнопку микрофона. Маскирующий сигнал формируется из речи участников переговоров, что обеспечивает максимальную комфортность переговоров. Он создается динамиками автомобильного приемника.

Офисный режим использования. Для работы в этом режиме используется обычный FM приемник. Перед проведением важного разговора приемник настраивается на частоту APD-M7 (88,3 МГц).

Это интересно знать.
По дисплею контролируйте, чтобы была набрана именно эта частота.

Приемник устанавливается так, чтобы создать максимальный маскирующий сигнал в месте предполагаемого нахождения диктофона или радиожучка. Его громкость предварительно выставляется таким образом, чтобы на диктофоне посетителя нельзя было разобрать слов хозяина помещения.

В процессе разговора хозяин помещения предупреждает посетителя о важности разговора и нажимает кнопку на микрофоне, подключенном к АПД-7М «Гюрза». Маскирующий сигнал представляет собой речь хозяина помещения, преобразованную по случайному закону. Так как уровень маскирующего сигнала пропорционален

громкости исходной речи, то это обеспечивает комфортность ведения переговоров. Если необходимо замаскировать голос второго собеседника, то в гнездо второго микрофона вставляется дополнительный микрофон.

Зарядка аккумулятора. Для зарядки аккумулятора, штекер зарядного устройства вставляется в гнездо второго микрофона. Зарядка производится до тех пор, пока светодиод индикации не погаснет.

Рубеж НГ — сетевой генератор шума для сетей 220 В

Назначение. Сетевой генератор шума «Рубеж НГ» предназначен для подавления подслушивающих устройств, использующих в качестве канала передачи сеть 220 В.

Технические характеристики:

- ширина спектра шума, кГц ..... 0,3—7000;
- спектральная плотность мощности в диапазоне 0,3—25 кГц, мВт/Гц ..... $0{,}3\times10^{-2}$;
- спектральная плотность мощности в диапазоне 25—95 кГц, мВт/Гц ..... $2{,}8\times10^{-2}$;
- спектральная плотность мощности в диапазоне 95—7000 кГц, мВт/Гц ..... $0{,}24\times10^{-3}$;
- потребляемая мощность, Вт 8,5;
- питание ..... 220 В, 50 Гц.

Внешний вид прибора представлен на **рис. 5.12.**

Рис. 5.12. Внешний вид прибора «Рубеж НГ»

Принцип действия. «Рубеж НГ» обеспечивает генерацию шума в диапазоне частотного спектра от 300 Гц до 7 МГц. В наиболее часто используемом диапазоне частот от 25 кГц до 95 кГц генератор обеспечивает максимальный уровень спектральной плотности мощности шумового сигнала. К краям диапазона уровень спектральной плотности мощности плавно снижается. Помеха подается в сеть 220 В по шнуру питания. Изделие не создает помех устройствам бытовой электроники.

Включение изделия. Сетевая вилка генератора шума «Рубеж НГ» включается в сеть 220 В. На передней панели изделия включается тумблер. Загорание индикаторной лампочки свидетельствует о включении.

Будьте осторожны.
Не допускается включение генератора шума в специальные удлинители с помехоподавляющими фильтрами, так как в этом случае резко уменьшается уровень шумовой помехи в сети. Генератор должен быть включен до удлинителя с фильтром.

Хамелеон XL — подавитель диктофонов

Назначение. Предотвращение записи беседы на диктофон посетителем. Акустическое подавление жучков в средствах связи и коммуникациях. Может использоваться для одновременной маскировки речи двух человек.

Конструктивно мобильный подавитель диктофонов закамуфлирован под обыкновенные компьютерные колонки и может находиться на столе постоянно.

Это интересно знать.
Акустические подавители диктофонов в настоящее время являются единственными эффективными средствами защиты от всех видов прослушивающих устройств.

Технические характеристики:
- время работы приемной колонки в режиме средней громкости, ч.....3;
- время работы передающей колонки, ч 10;
- диапазон спектра маскирующего сигнала, Гц .....180—5400;
- уровень подавления сигнала акустозавязки, дБ.....28;
- время зарядки аккумуляторов, ч 18;
- расстояние между передающей и приемной колонками, м.. до 6;
- ток потребления приемной колонки при выключенной передающей колонке, мА.....22;
- емкость аккумуляторов в колонках, мА/ч .....600.

Внешний вид прибора представлен на **рис. 5.13.**

Состоит прибор из передающей колонки, приемной колонки, дополнительного микрофона, зарядного устройства и барсетки.

Принцип действия. Перед проведением важного разговора приемная колонка устанавливается так, чтобы создать максимальный маскирующий сигнал в месте предполагаемого нахождения диктофона или радиожучка. Ее громкость предварительно выставляется таким образом, чтобы

на диктофоне посетителя нельзя было разобрать слова хозяина помещения. После этого передающая колонка выключается красным тумблером, а приемная колонка остается включенной.

В процессе разговора хозяин помещения предупреждает посетителя о важности разговора и включает тумблер питания на передающей колонке.

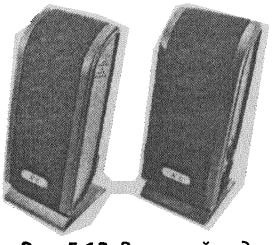


Рис. 5.13. *Внешний вид прибора «Хамелеон XL»*

Маскирующий сигнал представляет собой речь хозяина помещения, преобразованную по случайному закону. Так как уровень маскирующего сигнала пропорционален громкости исходной речи, то это обеспечивает комфортность ведения переговоров.

Это интересно знать.
Для максимальной маскировки речи разговор ведется в сторону передней панели передающей колонки.

Если необходимо замаскировать голос второго собеседника, то в гнездо для зарядки передающей колонки необходимо подключить дополнительный микрофон.

Если помещение небольшое (9—12 м^2), то мощности приемной колонки достаточно, чтобы подавить любые диктофоны и «жучки». Для перекрытия большей площади надо в боковое гнездо приемной колонки подключить дополнительную акустическую систему.

Зарядка аккумуляторов. Если в процессе работы зеленый светодиод на колонках начинает менять цвет на красный, то колонки необходимо зарядить. Для зарядки аккумуляторов штекер зарядного устройства вставляется в гнездо зарядки на задней стенке колонок. Процесс зарядки индицируется свечением светодиода на верхней панели зарядного устройства. Время заряда должно составлять 18—20 ч.

Особенности. Защищает от записи разговора на любые цифровые или аналоговые записывающие устройства. Изделие выполнено в корпусах компьютерных колонок, что позволяет его использовать без лишних вопросов со стороны окружающих людей. Удобство использования без лишних проводов за счет беспроводной связи и встроенных аккумуляторов. Имеется возможность подключения дополнительных колонок, для увеличения площади покрытия маскирующей акустической защиты. Прибор можно использовать и транспортировать без креплений, например, в портфеле или папке.

ГЛАВА 6

РАДИОМИКРОФОНЫ: РАЗРАБОТКА, СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ

Радиомикрофон поможет прослушать не только важные разговоры в закрытой комнате, но и даст возможность маме услышать плачь грудного ребенка и прийти ему на помощь. Без радиомикрофонов не обходится сейчас ни один концерт. В этом разделе представлено множество простых и полезных схем радиомикрофонов. Они систематизированы по принципу от «простого к сложному». Большинство конструкций могут изготовить радиолюбители, не обладающими значительным опытом и без использования сложной измерительной аппаратуры.

Назначение радиомикрофонов

Рассмотренные в этой главе радиомикрофоны достаточно эффективны и надежны. Каждая из схем демонстрирует интересные схемотехнические и конструктивные решения использующиеся при разработке радиомикрофонов.

При изготовлении схем на частоты более 100 МГц приходится сталкиваться с тем, что конструктивное исполнение устройства и применяемые компоненты значат гораздо больше, чем его принципиальная схема.

В этом же разделе рассмотрены средства борьбы с использованием радиомикрофонов, в тех случаях, когда это необходимо:

- **во-первых**, радиомикрофон можно обнаружить и ликвидировать;
- **во-вторых**, ему можно поставить активную помеху, сделав его использование мало эффективным.

Простейший радиомикрофон на двух транзисторах

Эта наиболее распространенная схема жука, которую можно встретить в Интернете. Отличается простотой сборки и настройки, малыми размерами, а также своей не очень высокой стабильностью. Ее автор Андрей Мартынов (http://cxem.net/radiomic/radiomic.php) называет схему «Жучок для начинающих», т. е. новичкам он рекомендует начинать творчество именно с нее.

Все используемые детали — в SMD корпусах (размер 0805), но для начала можно взять элементы в корпусе 1206.

Совет.

Между плюсом и минусом питания (параллельно батарейке) нужно поставить конденсатор емкостью 0,01 мкФ.

Катушка должна иметь 5 витков провода диаметром 0,5 мм на оправке диаметром 4—5 мм (возьмите стержень от гелевой ручки) Питание — батарейка «Крона» 9 В. Антенна — кусок провода, длиной 40 см. Принципиальная схема устройства и его печатная плата приведены на **рис. 6.1**.

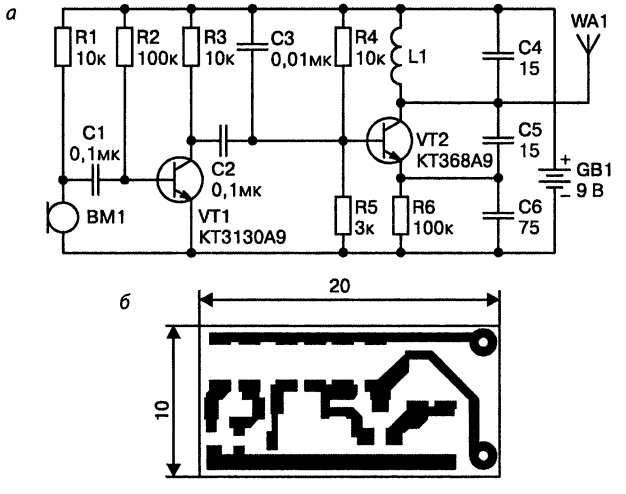


Рис. 6.1. *Радиомикрофон для начинающих: а — принципиальная схема; б — печатная плата*

Настройка схемы производится так. Включить FM радиоприемник, установить частоту примерно 96 МГц. Подключить питание. Покрутить слегка ручку настройки приемника влево-вправо. Если себя плохо слышите:

- поищите еще;
- посжимайте или порастягивайте катушку.

Если при включении передатчика в приемнике не слышно изменений, то может быть две причины:

- ошибочный монтаж;
- неисправен второй транзистор.

Если плохо слышно, то можно подобрать вместо резистора (на плате в верхнем левом углу 10 кОм) другой или заменить первый транзистор.

Для уменьшения размеров можно использовать микрофон минимального размера, но все равно батарейка «Крона» будет определять размер всего изделия.

Радиомикрофон на одном биполярном транзисторе

Рассмотрим еще один простейший радиомикрофон (**рис. 6.2**). Он собран на транзисторе КТ3107Б, можно использовать КТ3107БМ. К коллектору транзистора VT1 надо припаять кусок провода длиной 37 см. В качестве источника питания можно использовать литиевую «таблетку» на 3 В. Катушка содержит 6 витков провда 0,5 мм, ее можно намотать на стержне от гелевой ручки.

После включения схема должна работать сразу. **Способ настройки** такой же, как у предыдущей схемы.

Совет.

Если частота передатчика лежит ниже диапазона 88—108 МГц, то надо поставить конденсатор С2 на 30 пФ.

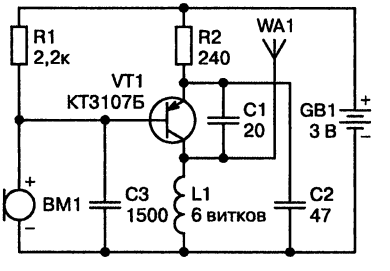


Рис. 6.2. Схема простейшего радиомикрофона на КТ3107Б

Радиомикрофон на транзисторе, включенном по схеме с трансформаторонй связью

Эта схема обеспечивает дальность передачи сигнала до 100 м при сохранении хорошей акустической чувствительности. Это достигается благодаря включению транзистора по схеме с трансформаторной связью (схема Майсснера). Это позволяет регулировать все параметры только сжатием/растяжением витков катушек! Рабочая частота — 94 МГц. Схема радиомикрофона представлена на **рис. 6.3**.

Конструктивно схема выполняется как насадка на батарейку «Крона». Весь монтаж производится прямо на панельке от использованной «Кроны».

Катушка L1 содержит 6 витков провода ПЭВ-0,5 на стержне от шариковой ручки (3—4 мм). **Катушка L2** содержит 3 витка провода ПЭВ-0,2 и наматывается поверх катушки L1 в том же направлении. **После сборки** потребляемый ток должен быть в пределах 10 мА.

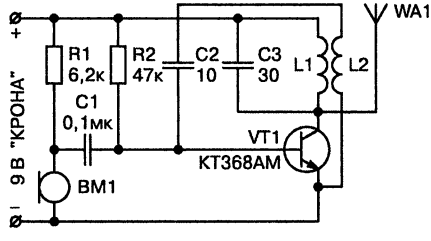


Рис. 6.3. *Радиомикрофон, собранный по схеме трехточки*

Совет.

Если ток больше, то надо подобрать величину резистора R2. Транзистор надо ставить с как можно большим коэффицентом усиления.

Затем нужно припаять антенну, в качестве которой служит кусок провода длинной 60 см. Потребляемый ток должен возрости, это свидетельствует о хорошей работе схемы.

Настройка схемы. Сжатием/растяжением витков L1 следует настроить передатчик на нужную частоту. После чего начать растягивать витки L2. При этом чувствительность микрофона должна возрастать.

Это интересно знать.

Растягиваем витки до максимальной чувствительности, при которой еще сохраняется генерация.

Окончательно подстроив частоту, заливаем катушку парафином или клеем. Для **повышения стабильности частоты** рекомендую подключать антенну через конденсатор 2—3 пФ, а также зашунтировать схему конденсатором 0,1 мкФ.

Радиомикрофон, собранный по схеме Хартли с нестандартным включением обратной связи

Этот жучок с высоким КПД собран по схеме Хартли (**рис. 6.4**) с нестандартным включением обратной связи, благодаря чему имеет КПД на 10—20% выше аналогичных схем. При длине антенны 20 см дальность действия достигает 140 м. Катушка L1 5+5 витков провода ПЭВ-0,5 мотается на оправке 3 мм.

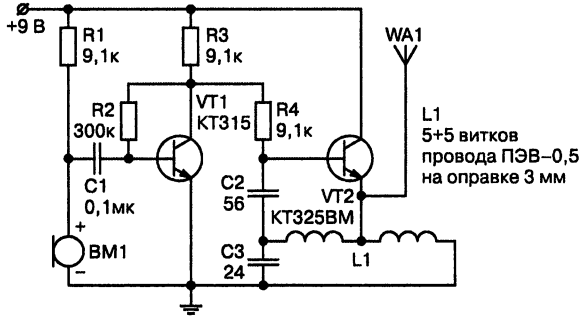


Рис. 6.4. *Принципиальная схема радиомикрофона, собранного по схеме Хартли*

Как правило, схема начинает работать сразу после сборки. Если в приемнике слышен писк, следует зашунтировать схему конденсатором емкостью не менее 1 мкФ.

Совет.

Антенну лучше подключить через конденсатор емкостью 1—2 пФ.

Радиомикрофон на полевом транзисторе с изолированным затвором

Данный радиомикрофон построен на полевом транзисторе с изолированным затвором (МОП-транзисторе) (**рис. 6.5**). Схему разработал и опубликовал А. Колтыков на сайте http://cxem.net.

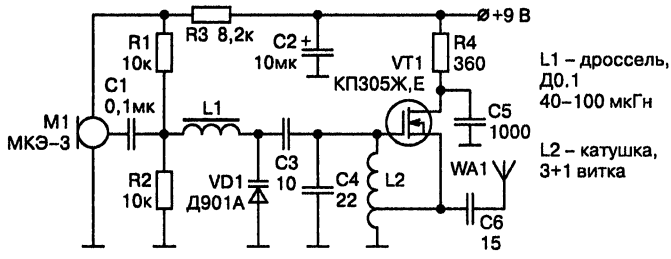


Рис. 6.5. Схема радиомикрофона на полевом транзисторе с изолированным затвором

При использовании источника питания 9 В данная схема обеспечивает дальность передачи (на частоте 74 МГц) 150—200 м на открытом пространстве при увствительности УКВ-приемника 10—15 мкВ. При этом ток потребления составляет 12—14 мА. Длина передающей антенны — 1 м.

Катушка L1 — это дроссель, например, Д0,1 индуктивностью 40—100 мкГн.

Катушка L2 (3+1 витка) — это бескаркасная катушка, имеющая внутренний диаметр 6 мм. Диаметр провода должен составлять 0,8 мм. Желательно использовать посеребренный провод.

Радиомикрофон на микросхеме К174ПС1

Схема этого радиомикрофона построена на микросхеме DA1 К174ПС1. В качестве **микрофона** в передатчике используется трехвыводный электретный микрофон BM1 (**рис. 6.6**). Его равноценно можно заменить двухвыводным по схеме, представленной на **рис. 6.7**. Радиомикрофон работоспособен в диапазоне напряжений питания от 4,5 до 9 В.

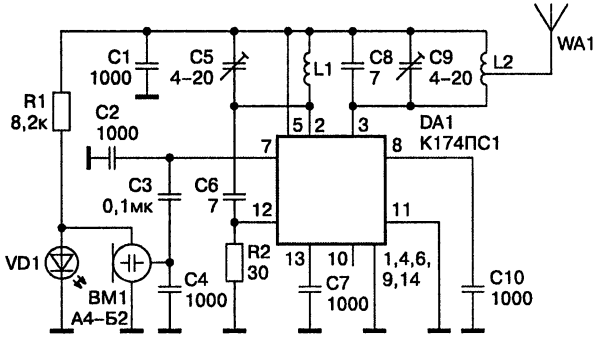


Рис. 6.6. Схема радиомикрофона на микросхеме К174ПС1

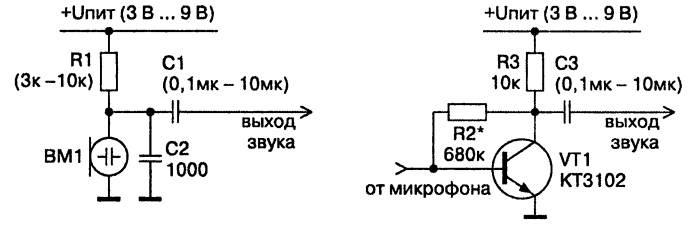


Рис. 6.7. Варианты включения в схему двухвыводного электретного микрофона

Это интересно знать.
Этот микрофон должен обладать достаточно большой отдачей по звуковому напряжению или иметь после себя один усилительный каскад на транзисторе.

Осуществление частотной модуляции без использования усилителя низкой частоты, варикапов и т. п. позволяет получить высокую линейность и большой динамический диапазон звукового сигнала с характеристиками ограниченными только свойствами микрофона. Благодаря этому схема имеет очень высокое качество звука.

Светодиод VD1 стабилизирует напряжение питания микрофона и является индикатором работы. Светодиод может быть любого типа с падением напряжения на нем 1,5—3 В или при применении двухвыводного микрофона отсутствовать.

Блокирующие конденсаторы номиналом 1000 пФ должны быть в исполнении для поверхностного монтажа или обычные, но с возможно более короткими ножками.

Катушки индуктивности L1, L2 — бескаркасные, имеют по пять витков каждая. Наматываются медным проводом диаметром 0,2—0,5 мм, например, на сверле.

Диаметр намотки составляет:

- 3,5 мм для диапазона 88—108 МГц;
- 2,5 мм для диапазона 100—140 МГц;
- 1,5 мм для диапазона 140—200 МГц.

Настройка передатчика заключается в установке требуемой частоты подстроечным конденсатором C5. Затем подстройкой C9 нужно добиться максимальной мощности излучения.

Степень включения антенны в выходной контур можно подобрать экспериментально по наилучшей стабильности и отдаваемой мощности. При изменении мощности передатчика резистором R2 (**рис. 6.6**) возможно потребуется изменить емкость конденсатора обратной связи C6. Емкость следует увеличивать при уменьшении номинала резистора R2.

Радиомикрофон, построенный на линии с распределенными параметрами

Такую схему можно встретить во многих изданиях, ведь он выполнен по классической схеме LC генератора с общей базой. Для звукового сигнала микрофона схема представляет собой повторитель напряжения и модулирует частоту контура L1, C4 изменением выходной емкости транзистора. Включение генератора по схеме с общей базой делает ненужным применение варикапа для создания частотной модуляции, но схема требует стабильного питающего напряжения.

Применение в такой конструкции обычного LC контура и обычных деталей может привести к генерации схемой непредсказуемого пучка частот. Однако, соблюдая некоторые правила конструирования высокочастотных конструкций, можно добиться неплохих результатов. Самым главным является выбор элемента, задающего частоту.

Одна из конструкций радиомикрофона, схема которого приведена на **рис. 6.8**, показана на **рис. 6.9**. Она представляет собой плату из одностороннего фольгированного стеклотекстолита размерами 45×30 мм, помещающуюся в спичечный коробок.

Катушка L1 представляет собой выполненную печатным способом линию. Элемент питания GB1 прижимается к поверхности «+» припаянной подпружиненной стальной скобкой XT1, которая служит минусовым контактом.

При использовании в качестве элемента питания щелочного элемента типа AG13 напряжением 1,5 В схема будет излучать на частотах около 420 МГц (подстраивается C4). При использовании литиевой трехвольтовой «таблетки» частота передачи будет около 610 МГц.

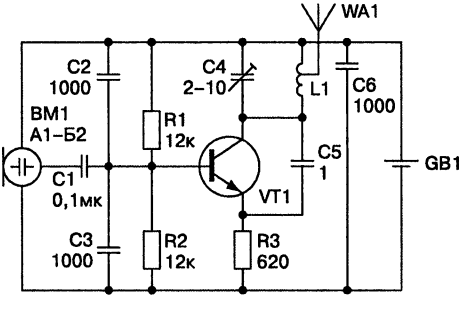


Рис. 6.8. Схема радиомикрофон на линии с распределенными параметрами

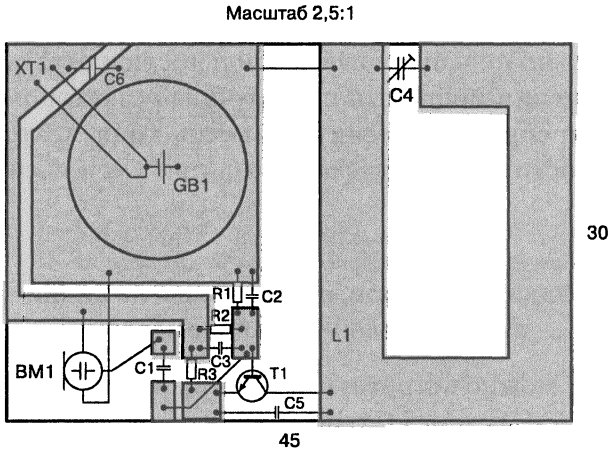


Рис. 6.9. Печатная плата

Такой передатчик удобно использовать как подопытный для поиска «жучков». Транзистор генератора желательно взять с граничной частотой не менее 4—10 ГГц. Из доступных отечественных транзисторов для этой цели хорошо подходят КТ640, КТ642, КТ647, КТ648, КТ657.

Резисторы и блокировочные конденсаторы — в исполнении для поверхностного монтажа. Микрофон желательно взять с наименьшей чувствительностью.

Печатная линия L1 одновременно служит антенной, транзистор VT1 включен в часть контура и не шунтирует его.

Это интересно знать.
Подобную конструкцию в действии можно увидеть, разобрав пульт недорогой автомобильной сигнализации.

Микромощный радиомикрофон с двумя рамками

Рассмотрим микромощный радиомикрофон с двумя рамками. Одна из простых схем (**рис. 6.10**) придумана неизвестным гением и распространена во множестве разновидностей.

Транзисторы VT1, VT2 совместно с контуром L1, C2 образуют автогенератор, ток питания которого стабилизирован внутренним полевым транзистором в электретном микрофоне BM1. С одной стороны, частота генератора не зависит от напряжения источника питания. А с другой стороны, ток, задаваемый и модулируемый микрофоном, соз-

дает частотную модуляцию генератора за счет изменения выходных емкостей транзисторов VT1, VT2.

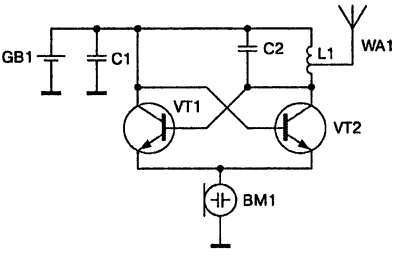


Рис. 6.10. Схема микромощного радиомикрофона

Ток передатчика задается резисторами R3, R4. Частота передачи модулируется звуковым сигналом через регулятор R1 и цепочку R2, C3. Катушка L1 содержит семь витков провода диаметром 0,8 мм, намотанного на оправке диаметром 3,5 мм с отводом от середины. Стабилизатор напряжения или тока в устройстве отсутствует, так как при низком потреблении тока устройством и использовании элемента типа АА напряжение элемента питания долгое время не будет изменяться.

Конструктивное исполнение схемы (**рис. 6.11**) предусматривает вместо сосредоточенных LC контуров применение линий с распределенными параметрами, которые одновременно служат антенной. Линии L1, L2 должны быть изготовлены из провода диаметром 0,3—0,7 мм и иметь одинаковую длину. При соблюдении указанных размеров и компонентов (форма рамок может быть любой) радиомикрофон стабильно работает на частоте около 94 МГц при напряжении питания от 1,5 до 12 В.

Частота его излучения слабо зависит от расположения внешних предметов, мощность достаточна для приема сигнала через 2—3 стены на бытовой ЧМ радиоприемник.

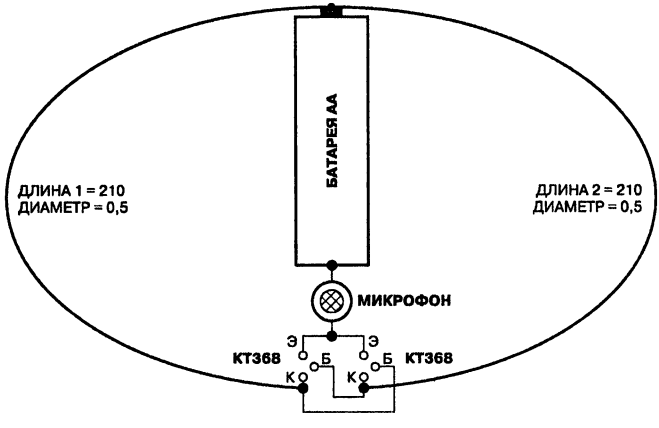


Рис. 6.11. Конструкция стабильного микромощного радиомикрофона

Это интересно знать.

Размер рамок можно уменьшить, подключив параллельно им конденсаторы емкостью несколько пикофарад. В этом случае стабильность частоты и дальность передачи будут меньше.

Применение. Эту конструкцию совместно с любым ЧМ приемником удобно использовать в качестве «радионяни», для реагирования на голос находящегося в другой комнате малыша.

Совет.

Можно уменьшить размеры рамок до длины 30—40 мм каждая, используя аккумулятор «таблетку» на 1,5 В и СВЧ транзисторы передатчик превращается в «жучка» с частотой передачи около 400—600 МГц и радиусом действия 5—10 м. С такими крошечными размерами и малой излучаемой мощностью возможность его нахождения любыми видами техники становится случайной.

Радиомикрофон со схемой стабилизации ПАВ резонатором и с автопуском

Схема представляет собой образец коммерческой схемы радиомикрофона со стабилизацией ПАВ резонатором. Она снабжена акустопуском (см. **рис. 6.12**).

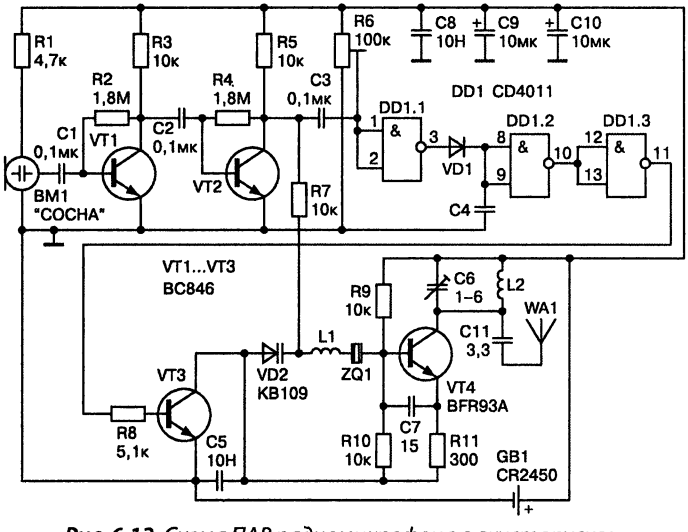


Рис. 6.12. Схема ПАВ радиомикрофона с акустопуском

Сигнал микрофона BM1 (трехвыводного или двухвыводного) усиливается двумя транзисторами VT1, VT2 и поступает одновременно:

- на модулирующий варикап VD2;
- систему акустопуска выполненную на КМОП инверторах микросхемы DD1 и ключе VT3.

На элементах DD1.1, VD1, C4 выполнен пиковый детектор звукового напряжения, подстроечный резистор R6 задает линейный режим работы элемента DD1.1 с сохранением его высокого входного сопротивления (устанавливается на половину напряжения питания).

Последовательно включенные элементы DD1.2, DD1.3 исполняют роль компаратора. Время удержания напряжения пиковым детектором (для того, чтобы передатчик не выключался во время коротких пауз) зависит в основном от времени саморазряда конденсатора C4, поэтому он может быть небольшой емкости 1—10 нФ.

Через ключ на транзисторе VT3 включается высокочастотный генератор на транзисторе VT4, стабилизированный ПАВ резонатором ZQ1. Для большего сдвига ПАВ резонатора по частоте последовательно с ним включена катушка L1. **Катушка** L1 имеет 6 витков проводом 0,3 мм на оправке 1,5 мм.

Катушка L2 имеет 4 витка проводом 0,4 на оправке 2 мм.

Совет.
Диод VD1 желательно взять с небольшим прямым падением напряжения — германиевый или Шотки.

Радиомикрофон с ЧМ модуляцией, выполненный на ТТЛШ четырехвходовом элементе И-НЕ с триггером Шмитта

На **рис. 6.13** показана схема радиомикрофона с ЧМ модуляцией, который выполнен на ТТЛШ четырехвходовом элементе И-НЕ с триггером Шмитта. Три логических входа элемента подключены к нагруженному емкостью выходу и обеспечивают высокочастотную генерацию элемента.

Четвертый вход питает и одновременно снимает звуковое напряжение с электретного микрофона.

Этим обеспечивается частотная модуляция, поскольку «висячий» вход ТТЛ читается как «1», а на нем присутствует напряжение около 1,5 В.

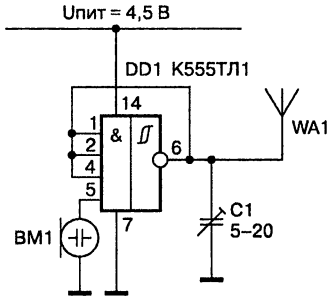


Рис. 6.13. Принципиальная схема УКВ ЧМ передатчика на логическом элементе

При указанной емкости конденсатора С1 устройство работает в диапазоне 80—100 МГц, частота настройки регулируется подстроечным конденсатором С1. Антенной служит отрезок медного провода длиной 10—30 см. Но стабильность частоты этого передатчика оставляет желать лучшего.

Микромощный радиомикрофон без катушек индуктивности, построенный на микросхеме 155ЛА3

Микромощный радиопередатчик, не имеющий катушек индуктивности, на диапазон 66—100 МГц, можно построить на микросхеме 155ЛА3. Дальность действия такого передатчика будет составлять 50—100 м. А его сигнал можно услышать на обычном УКВ приемнике.

Схема передатчика приведена на **рис. 6.14**. Сигнал с микрофона BM1 подается на вход (выводы 1 и 2) генератора, собранного на элементах DD1.1, DD1.4. На выходе (вывод 11) генератора получаются модулированные высокочастотные колебания, которые излучаются антенной WA1 в пространство. Настройка передатчика на требуемую частоту производится резистором R1. Для стабильной работы передатчика при изменении питающего напряжения в его схеме имеется стабилизатор напряжения, собранный на транзисторах VT1 и VT2.

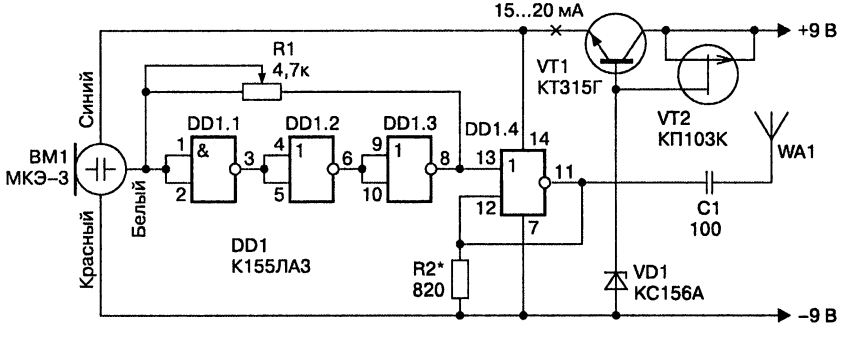


Рис. 6.14. Схема радиомикрофона на микросхеме 155ЛА3

Питание передатчика осуществляется от источника с напряжением 6—9 В. Можно использовать батарею типа «Крона» или 4 элемента типа 316. В качестве антенны WA1 передатчика можно использовать металлический штырь длиной около 1 м или телескопическую антенну от радиоприемника.

Настройка передатчика начинается с установки резистором R2 тока 15—20 мА (место на схеме показано крестиком). Далее, включив УКВ приемник, нужно устанавить указатель его настройки в том месте шкалы, где не слышны радиовещательные станции. Произнося слова в микрофон, настройкой резистора R1 следует добиваются уверенного приема.

Полное описание устройства приводится на http://cxem.net/radiomic/radiomic.php.

Радиомикрофон с питанием от сети 220 В и использующий в качестве антенны провода этой сети

Основное достоинство этого радиомикрофона в том, что он **питается от сети 220 В**, а в качестве антенны **использует провода этой же сети**. Приемник принимает сигналы либо через антенну, либо через специальный сетевой адаптер. Схема устройства приведена на **рис. 6.15.**

Блок питания радиопередатчика бестрансформаторный, напряжение сети поступает на дроссели Др1 и Др2, а затем на конденсатор С2, на котором гасится излишек напряжения. Переменное напряжение выпрямляется мостом VD1, нагрузкой которого является стабилитрон VD2 типа КС510А. Пульсации напряжения сглаживаются конденсатором С3.

Модулирующий усилитель выполнен на транзисторе VT1 типа КТ315. С его коллектора напряжение через резистор R2 поступает на варикап VD3 типа КВ109А, изменение емкости которого и осуществляет частотную модуляцию.

Задающий генератор передатчика выполнен по схеме индуктивной трехточки на транзисторе VT2 типа КТ315.

Частота генератора определяется элементами L1, C5, C4, VD3. Обратная связь осуществляется через конденсатор С7. Режимы транзисторов VT1 и VT2 по постоянному току регулируются резисторами R5 и R4, соответственно. Напряжение смещения транзисторов формиру-

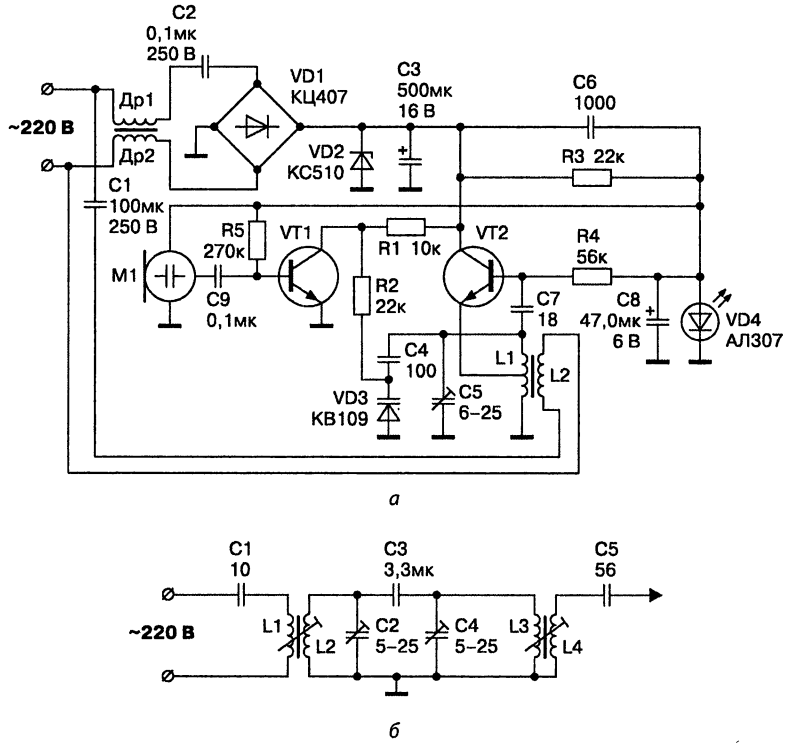


Рис. 6.15. *Радиомикрофон с передачей сигнала по сети 220 В:*
а — принципиальная схема радимикрофона; б — специальный приемный адаптер

ется из напряжения параметрического стабилизатора, выполненного на резисторе R3, светодиоде VD4 и конденсаторе C8. Напряжение высокой частоты с катушки L2 поступает в сеть через конденсатор C1.

Дроссели Др1 и Др2 намотаны на каркасах от ВЧ катушек переносных приемников и содержат по 100 витков провода ПЭВ 0,1 мм. Катушки L1 и L2 намотаны на малогабаритных каркасах диаметром 5 мм и высотой 12 мм с подстроечными сердечниками из феррита.

Для диапазона 27 МГц катушка L1 имеет 10 витков с отводом от середины, а катушка L2 имеет 2 витка провода ПЭВ 0,3 мм.

Конденсаторы C1 и C2 должны быть на напряжение не менее 300 В. Диодную сборку КЦ407А можно заменить простыми диодами типа КД105, КД208. Вместо стабилитрона VD2 можно применить любой другой с напряжением стабилизации 8—12 В.

Для приема сигналов этого передатчика применяется специальный адаптер, схема которого представлена на **рис. 6.15, *б***.

Катушки L2—L4 и конденсаторы C2—C4 образуют двухконтурный ФСС. Катушки L1—L4 намотаны на каркасах от ВЧ катушек переносных приемников, содержат 2, 14, 14 и 5 витков, соответственно, проводом ПЭВ 0,23 мм. Конденсатор C1 на напряжение 300 В, C2 и C4 — подстроечные.

Будьте осторожны.
При работе с этими устройствами соблюдайте правила и меры безопасности, т. к. элементы устройств находятся под напряжением 220 В!

Миниатюрный средневолновый радиомикрофон с амплитудной модуляцией

А теперь создадим **миниатюрный средневолновый радиомикрофон** с амплитудной модуляцией. Схема АМ передатчика (**рис. 6.16**) на двух транзисторах позволяет создать простой передатчик для экспериментов с радиомикрофоном. Рабочий диапазон частот передатчика составляет 500—1500 кГц. Его **достоинством** является то, что диапазон средних волн, в котором он работает, в настоящее время практически пуст, в отличие от УКВ диапазона 88—108 МГц, где в городах сейчас «яблоку негде упасть» от сигналов мощных вещательных станций. Поэтому дальность распространения, качество сигнала можно спокойно оценить без опасения, что сигнал будет забит мощной помехой, на которую система автоподстройки УКВ приемника так и норовит подстроиться.

В качестве приемника можно использовать любой — от ламповой радиолы до цифрового тюнера, имеющий диапазон средних волн (СВ или MW).

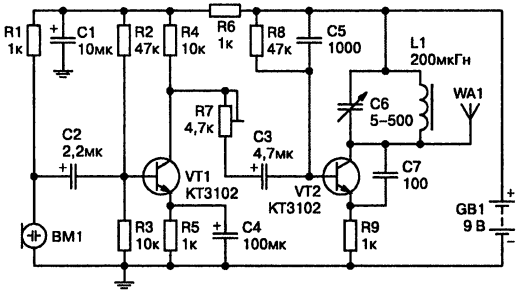


Рис. 6.16. Схема средневолнового радиомикрофона с амплитудной модуляцией

На транзисторе VT1 выполнен классический УНЧ с общим эмиттером, который усиливает сигнал электретного микрофона BM1. Через регулятор глубины модуляции на резисторе R7 сигнал поступает на базу автогенератора VT2, выполненного по схеме с общей базой.

Для сигналов звуковой частоты VT2 включен по схеме с общим коллектором, ток звуковой частоты через него пропорционален величине входного НЧ сигнала. Конденсатор C5 заземляет базу транзистора VT2 по высокой частоте, конденсатор C7 обеспечивает обратную связь для работы автогенератора.

Катушка L1 может быть любой, в том числе и стандартным дросселем. В качестве антенны WA1 используется изолированный провод возможно большей длины. Если L1 выполнить на ферритовом стержне (например, диаметром 8 мм длиной 100 мм магнитной проницаемостью 600НН, как магнитную антенну средневолнового приемника), то такая антенна, в отличие от длинного провода, будет обладать выраженными направленными свойствами.

Беспроводной скрытый наушник

Рассмотрим **беспроводной скрытый наушник.** Это изделие разработано умельцами с **www.vrtp.ru** и дает фору подобным устройствам, в том числе различным гарнитурам типа «блютус» по себестоимости, экономичности, незаметности и совместимости с различной техникой.

Устройство, принципиальная схема которого представлена на **рис. 6.17, *а***, работает на принципе индуктивной связи между катушками передатчика и приемника на звуковых частотах.

Собственно сам передатчик состоит только из одной передающей катушки, которая наматывается на оправке диаметром 20 см (подходящая кастрюля) и содержит не менее 50 витков изолированного провода диаметром 0,2 мм. Затем провод снимается, и обматывается каким-либо изолирующим материалом (хотя бы малярным скотчем), чтобы получилось плотное кольцо.

Выводы катушки подпаиваются к гибкому монтажному проводу длиной около полуметра со штеккером (например, «джек» 3,5 мм моно) для подключения к источнику звука.

Сопротивление провода такого диаметра и длины составит 15—20 Ом, что равноценно сопротивлению обмоток обычных наушников. Поэтому такую катушку можно подключать к выходу любой техники, куда подключаются головные телефоны (наушники).

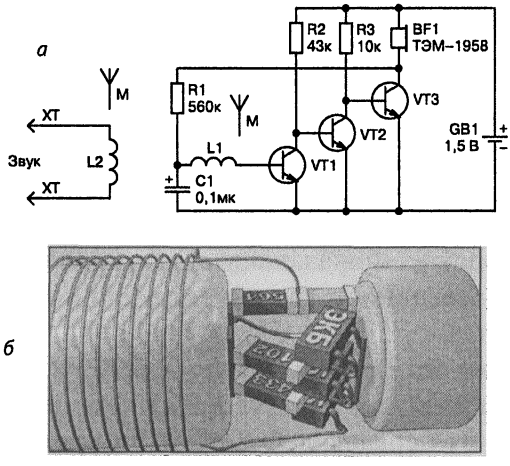


Рис. 6.17. *Беспроводный наушник скрытного ношения:*
а — схема радионаушника;
б — внешний вид монтажа радионаушника в миниатюрном исполнении

Основой миниатюрного приемника является динамический телефон ТЭМ-1958 (или аналогичный) от слуховых аппаратов. Если не требуется, чтобы приемник был совершенно невидим, то в качестве звукового капсюля можно применить любой динамический телефон с сопротивлением обмотки не менее несколько десятков ом.

Приемник представляет собой трехкаскадный усилитель низкой частоты с непосредственной связью между каскадами и обратной связью по постоянному току через резистор R1.

Коэффициент усиления такого УНЧ будет равняться отношению сопротивления R1 к входному сопротивлению транзистора VT1. То есть коэффициент усиления будет огромным.

Схема охвачена обратной связью по постоянному току и не нуждается в настройке. Подобные схемы с минимальным числом радиоэлементов публиковались еще во времена первых транзисторов и работают до сих пор уже на элементной базе для поверхностного монтажа.

Схема собирается объемным монтажом с применением резисторов и транзисторов в исполнении для поверхностного монтажа (если требуется миниатюрность).

Катушка приемника L1 наматывается на телефоне BF1 и содержит 70—100 витков провода диаметром 0,05—0,07 мм (так чтобы влезало в ухо). Радиоэлементы расположены между телефоном и батареей питания (элемент питания для часов GB1, см. **рис. 6.17, *б***).

Далее вся конструкция обтягивается термоусадочной трубкой. Транзисторы VT1—VT3 — BC847 (в корпусе COT323), или отечественные КТ3130 А9. Транзисторы могут быть любыми миниатюрными, в том числе и p-n-p типа (со сменой полярности батареи питания).

Правильно собранный приемник должен издавать слабое шипение и реагировать на приближение к сетевым трансформаторам (ловить фон 50 Гц).

Для эксплуатации наушника кольцо антенны передатчика надевают на шею, штекер подсоединяется к приемнику или сотовому телефону, наушник вставляется в ухо.

Можно заметить, что в этом случае оси катушек передатчика и приемника перпендикулярны друг другу. Это ухудшает передачу звукового сигнала от передающей катушки к приемной. Чтобы усилить связь между катушками, можно поэкперементировать с положением на шее катушки передатчика или попробовать применить катушку передатчика на ферритовом стержне, размещаемую на плече (**www.vrtp.ru**).

Рассмотрим еще несколько полезных схем.

Миниатюрный радиопередатчик на биполярных транзисторах

Схема радиопередатчика (www.compradio.nm.ru и http://radiolla.narod.ru/sh_juk_100m.htm) показана на **рис. 6.18.** Можно кого-нибудь подслушивать, сдавать экзамен; всех возможностей и не перечислить. Главным его достоинством являются его маленькие размеры.

Желательно нарисовать схему расположения деталей на плате. Лучше всего использовать тонкий слой картона толщиной не более 1 мм. Детали располагать как можно ближе друг к другу, чтобы размеры были поменьше.

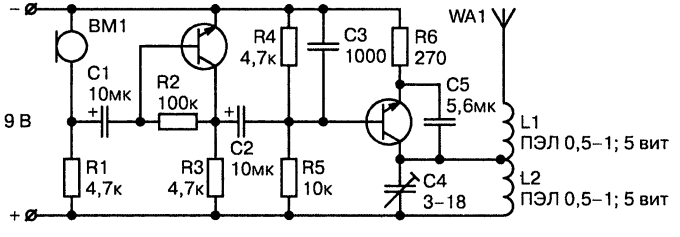


Рис. 6.18. Принципиальная схема радиопередатчика

Принимать сигнал жука лучше всего на FM-сканеры, так как в процессе длительной работы частота передаваемой волны может понижаться, а сканеры продолжают держать эту волну. В общем, самое время взглянуть на схему **рис. 6.18**.

Это интересно знать.
Состоит данное устройство из 2 частей: усилитель ЗЧ и задающий генератор. Если в схему добавить усилитель мощности, то дистанцию можно будет увеличить до 1 км.

Сначала собираем УЗЧ (микрофон, 2 резистора по 4,7 кОм, и один на 100 кОм, а также транзистор и емкость 10 мкФ). Затем нужно все проверить — присоединить наушники к отрицательному выводу конденсатора и к минусу всей схемы. Не забудьте подключить батарейку.

Затем что-нибудь проговорите в микрофон — в наушниках можно услышать. Далее нужно собрать задающий генератор (то есть достраиваете схему до конца).

Детали. Резисторы: 10 кОм, 4,7 кОм, 270 Ом. Конденсаторы: 10 мкФ, 1 нФ, 5,6 пФ, и переменная емкость, работающая в диапазоне от 3 до 18 пФ. Но ее вполне можно заменить постоянной емкостью, емкость которой попадает в этот промежуток (3—18 пФ). Транзисторы можно применить такие: С945 или КТ3102 — левый на схеме; КТ3102 — правый на схеме. Катушки индуктивности можно намотать на стержне обычной шариковой ручки из медного провода диаметром от 0,5 до 1 мм. В каждой катушке сделать по 5 витков.

Антенна — кусок провода или еще что-нибудь похожее на это длиной 70 см. Микрофон можно взять малогабаритный «Сосна», также работает и с ДЭМШ 1-А.

Радиомикрофон мощностью 200 мВт

Схема радиопередатчика мощностью 200 мВт (http://sima0607.se-ua.net/page 69) показана на **рис. 6.19.**

Сигнал от электретного микрофона Ml типа МКЭ-3 поступает на двухкаскадный низкочастотный усилитель с непосредственными связями на транзисторах VT1, VT2 типа КТ315. Рабочая точка усилителя устанавливается автоматически цепью обратной связи по постоянному току через R5, R6, C3.

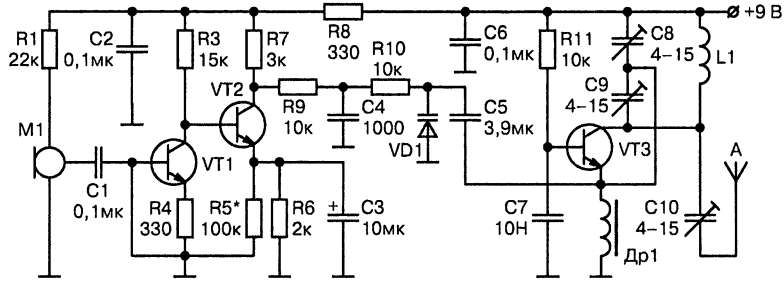


Рис. 6.19. *Радиопередатчик на 200 мВт*

Усиленный низкочастотный сигнал с коллектора транзистора VT2 через фильтр низкой частоты на элементах R9, C4 и резистор R10 поступает на варикап VD1 типа КВ109, включенный в эмиттерную цепь транзистора VT3 типа КТ904. Напряжение смещения на варикап VD1 задается коллекторным напряжением транзистора VT2.

Однокаскадный ВЧ генератор выполнен на транзисторе VT3. Напряжение смещения на базе этого транзистора задается резистором R11. Транзистор VT3 включен по схеме с общей базой. В его коллекторной цепи включен контур C8, C9, L1. Частота настройки генератора определяется индуктивностью катушки L1 и емкостями C8, C5, VD1. Конденсатор C9 устанавливает глубину обратной связи, а конденсатор C10 согласует контур с антенной.

Детали. Все детали передатчика малогабаритные. Дроссель Др1 типа ДПМ 0,1 на 60 мкГн. Дроссель можно заменить на самодельный, намотанный на резисторе МЛТ-0,25 сопротивлением более 100 кОм проводом ПЭВ 0,1 — 100 витков.

Катушка L1 — бескаркасная, с внутренним диаметром 8 мм, имеет 7 витков провода ПЭВ 0,8 мм. Компактная катушечная антенна выполнена тем же проводом, ее общая длина составляет 50 см. Катушка имеет диаметр 3 см.

Совет.

Если используется обычная антенна, то это провод или штырь должен быть длиной 0,75—1,0 м.

При настройке прибора конденсатором C8 настраивают радиомикрофон на свободный участок УКВ ЧМ диапазона. Конденсаторами C9 и C10 настраивают генератор на максимальную дальность связи.

Мощность передатчика составляет около 200 мВт. Если такая мощность не нужна, то ее легко понизить, увеличив вместе с тем срок службы источника питания. Для этого нужно увеличить сопротивление резистора R11 до 68—100 кОм и заменить дроссель Др1 на постоянный резистор сопротивлением 180—330 Ом.

Это интересно знать.
Так как в этом случае мощность радиомикрофона будет около 10 мВт, то транзистор VT3 можно заменить на КТ315 или КТ3102.

Транзисторы VT1, VT2 могут быть заменены на КТ3102, а транзистор VT3 — на КТ606, КТ907. Для питания устройства используется батарея на 9 В типа «Крона», «Корунд» или аккумулятор 7Д-0,15.

Жучок-радиомикрофон на биполярных транзисторах

Поверх жука на схеме (**рис. 6.20**) приклеивается «крышка» из десятка склеенных вместе листиков, а поверх нее — десятка три (можно больше, по ситуации) обычных листиков — «отрывай не хочу» (акустическая чувствительность схемы это позволяет). Когда листики закончатся и доберутся до «крышки» — решат что блок с браком, листочки склеены вместе и отправят жука в мусорку, что не так плохо, ибо факт прослушки обычно лучше не афишировать. Подробности см. на http://vrtp.ru/index.php?CODE=article&act=categories&article=1779

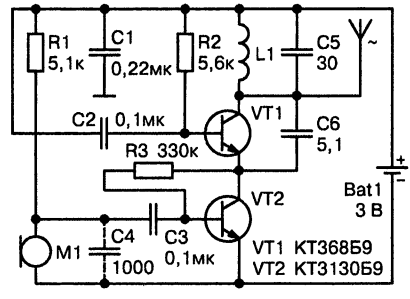


Рис. 6.20. Схема жучка-радиомикрофона

Чувствительный усилитель для прослушивания речи

Схема чувствительного усилителя для прослушивания речи показана на **рис. 6.21.** Устройство содержит двухкаскадный усилитель низкой частоты на малошумящих транзисторах VT1 и VT2, корректирующий фильтр на транзисторе VT3 и оконечный усилитель, собранный по двухтактной бестрансформаторной схеме, на транзисторах VT4—VT6. Акустическое усиление сигнала звуковой частоты, приведенным устройством составляет 85 дБ, начальный ток потребления — 1,8 мА,

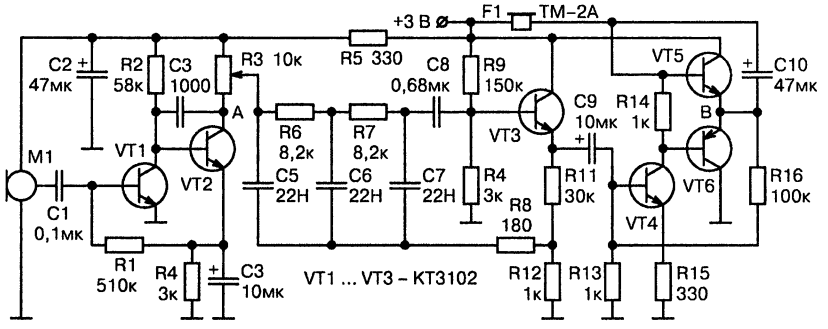


Рис. 6.21. Чувствительный усилитель для прослушивания речи

полоса усиливаемых частот — от 0,3 до 3 кГц, максимальный выходной уровень сигнала — 124 дБ.

Сигнал с микрофона M1 типа «Сосна» через конденсатор C1 поступает на базу транзистора VT1. Поскольку чувствительность усилителя звуковой частоты ограничена внутренними шумами транзисторов, то для уменьшения шумов в первых каскадах усилителя использованы малошумящие транзисторы типа КТ3102.

Усилительные каскады на транзисторах VT1 и VT2 охвачены глубокой отрицательной обратной связью, которая позволяет обеспечить устойчивую работу каскадов и более линейную АЧХ. Нагрузкой второго каскада усилителя является переменный резистор R3, он же является и регулятором громкости. Сложный RC-фильтр, состоящий из элементов R3, C5, R6, C6, R7, C7 отсекает «шумовые» ВЧ составляющие, принимаемые микрофоном, и оставляет только сигналы в полосе частот до 4 кГц. Этот диапазон обеспечивает наибольшую разборчивость речевой информации.

С выхода фильтра сигнал поступает на оконечный усилитель звуковой частоты, выполненный на транзисторах VT4, VT5 типа КТ315 и транзисторе VT6 типа КТ361. Нагрузкой усилителя служит головной телефон типа ТМ-2А или ТЭМ. Резисторы в схеме используются типа МЛТ-0,125. Резистор R3 — СП 3-41 или другой небольших габаритов.

Настройка устройства сводится к подбору сопротивлений резисторов R1 и R16 для установки напряжения в точках A и B равным половине напряжения питания.

Передатчик с высокочастотным генератором

Схема передатчика с высокочастотным генератором (http://cxem.net) показана на **рис. 6.22.**

Основу этого устройства составляет схема высокочастотного генератора на туннельном диоде. Ток, потребляемый генератором от источника питания, составляет примерно 15 мА и зависит от типа туннельного диода. Тип туннельного диода может быть выбран, по усмотрению радиолюбителя, с током потребления не более 10—15 мА (например, диод АИ201А).

Генератор сохраняет свою работоспособность при напряжении источника питания 1 В и выше при соответствующем выборе рабочей точки резистором R2. Дроссель Др1 наматывается на резисторе МЛТ 0,25 проводом ПЭВ 0,1 и содержит 200—300 витков. Чтобы провод не соскакивал с резистора, он периодически смазывается клеем «Момент», БФ-2 или другим.

Индуктивность дросселя должна быть 100—200 мкГн. Дроссель может быть заводского изготовления. Катушка колебательного контура L1 выполнена без каркаса и содержит 7 витков провода ПЭВ 1,0 мм. Диаметр катушки 8 мм, длина намотки 13 мм. Катушка связи L2 так же, как и L1 — бескаркасная, намотана проводом ПЭВ 0,35 мм, 3 витка, диаметр катушки 2,5 мм, длина намотки — 4 мм. Катушка L2 располагается внутри катушки колебательного контура L1.

Настройка передатчика сводится к установке рабочей точки туннельного диода путем вращения движка подстроечного резистора R2 до появления устойчивой генерации и подстройке частоты колебаний конденсатором С4. Антенной является отрезок монтажного провода длиной примерно в четверть длины волны. Глубину модуляции можно изменять подбором сопротивления резистора R1. Сигнал этого передатчика можно принимать на телевизионный приемник.

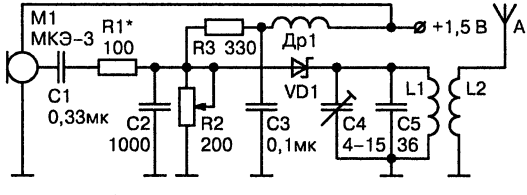


Рис. 6.22. Передатчик с высокочастотным генератором

Это интересно знать.

Значительно упростить конструкцию радиомикрофона можно при использовании малогабаритных конденсаторных микрофонов, включаемых непосредственно в колебательный контур высокочастотного генератора.

Мощность излучения вышеприведенных устройств составляет доли единиц милливатт. Соответственно, и радиус действия этих устройств составляет единицы — десятки метров.

Простой радиомикрофон на вещетельный диапазон 88—108 МГц

Простой радиомикрофон (http://shema.org.ua/index.php?name=News&op=Article&sid=513) представлен на **рис. 6.23.** Катушка L1 без каркаса содержит 4 витка посеребренного провода диаметром 1,5 мм (для диапазона 88—108,5 МГц). Антенну очень рекомендуется подключать через катушку связи (2 витка посеребренного провода диаметром 1,5 мм), расположенную рядом с L1.

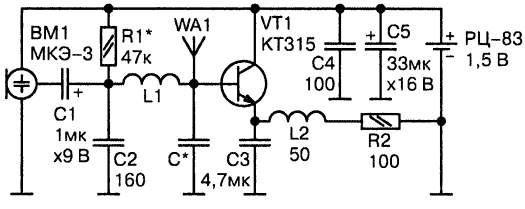


Рис. 6.23. *Простой радиомикрофон*

Дроссель имеет индуктивность 5—20 мкГн, можно применить самодельный, намотав на корпусе резистора МЛТ-0,125 сопротивлением не менее 500 кОм 40—50 витков провода ПЭВ-0.1, уложенных в один ряд. В качестве микрофона использован капсюль ТОН-2. Монтаж производится на двухстороннем фольгированом гетинаксе толщиной 1 мм.

Микропередатчик с ЧМ в диапазоне частот 80—100 МГц

Микропередатчик с частотной модуляцией в диапазоне частот 80—100 МГц (www.shema.org.ua) представлен на **рис. 6.24.**

Его выходная мощность — 0,5 мВт, потребляемый ток не превышает 2 мА. Питание осуществляется от аккумуляторного элемента

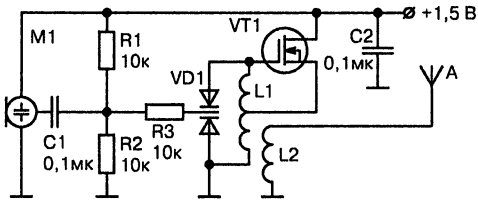


Рис. 6.24. Микропередатчик с ЧМ в диапазоне частот 80—100 МГц

напряжением 1,5 В. Задающий генератор УКВ диапазона выполнен на полевом транзисторе VT1 типа КП313А по схеме индуктивной трехточки с использованием проходной емкости МОП-транзистора.

Радиомикрофон с размещением колебательного контура в базовой цепи генератора, работающий по принципу «емкостной трехточки» с использованием частотной модуляции

Радиомикрофон, работающий в диапазоне частот 88—108 МГц (http://cxem.net/radiomic/radiomic35.php) представлен на **рис. 6.25**.

Особенность данного передатчика — размещение колебательного контура в базовой цепи генератора, работающего по принципу «емкостной трехточки» с использованием частотной модуляции.

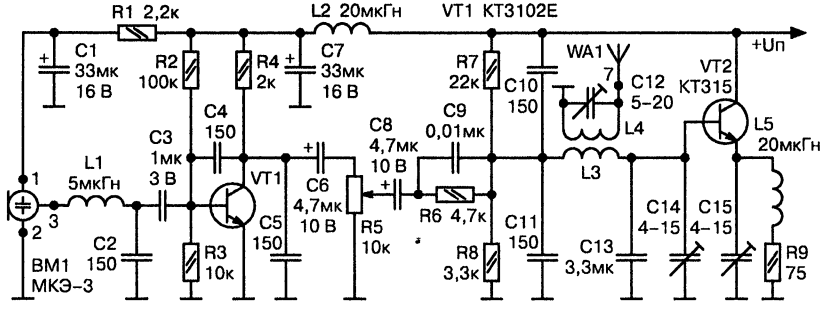


Рис. 6.25. Радиомикрофон в диапазоне 88—108 МГц

В его состав входят два блока: низкочастотный и высокочастотный. Применение в конструкции микрофонного усилителя, использование высокочувствительного микрофона (типа МКЭ-3, МД-27) и оптимальный выбор режима работы транзистора VT2 позволяют достичь требуемого значения глубины модуляции.

Схема обладает определенной универсальностью и может быть адаптирована в зависимости от требуемой конструкции и области

применения. Наличие **регулятора глубины модуляции** позволяет использовать передатчик для разных целей:

- как радиомикрофон для передачи речи;
- для подключения к различным источникам звука (телевизору, проигрывателю, магнитофону и т. д.) с целью ретрансляции их звукового сигнала на любой УКВ ЧМ радиоприемник.

Дальность действия радиомикрофона в зависимости от конструкции передающей и приемной антенн и класса радиоприемника может составить в помещении с железобетонными стенами несколько десятков метров, а при прямой видимости — не менее 0,5—0,6 км.

Микрофонный усилитель, построенный на одном транзисторе по схеме с общим эмиттером, предназначен для повышения чувствительности модулятора. В качестве VT1 желательно использовать малошумящий транзистор типа КТ3102. В коллекторную цепь транзистора включено сопротивление нагрузки R4. Напряжение смещения на базе VT1 определяется резисторами R2 и R3. Переменное сопротивление R5 регулирует глубину модуляции несущей частоты. Входное сопротивление микрофонного усилителя составляет порядка 300 Ом, поэтому в нем можно использовать практически любой низкоомный микрофон, однако для уменьшения габаритов конструкции предпочтение следует отдать миниатюрному МКЭ-3, МД-201 и им подобным.

Сигнал с коллекторной нагрузки транзисторов VT1 через регулятор R5 поступает в цепь низкочастотных предискажений R6C9. Она нужна для повышения помехозащищенности тракта передачи звука путем подъема уровня ВЧ составляющих звукового сигнала в передатчике и обратного действия, т. е. срезания ВЧ в радиоприемном устройстве.

Это интересно знать.

При использовании в системе связи отечественного радиоприемника постоянная времени для линейности АЧХ всего тракта должна составлять 50 мкс, а для импортного — 75 мкс. В последнем случае величины R6 и C9 составят 5,1 кОм и 0,015 мкФ, соответственно.

Для повышения качества звучания в области верхних частот (субъективного восприятия) можно применить и более высокое значение времени коррекции. Однако при значительном завышении данных номиналов происходит не только резкое подчеркивание высоких частот в принимаемом сигнале, но и вырастает уровень шума.

Отсутствие RC-цепи в передающем устройстве приведет к «глухому» звучанию приемника.

В качестве цепи НЧ предискажений можно применить простейший **регулятор тембра**. Этот регулятор позволяет изменять соотношение НЧ 100 Гц и ВЧ 10 кГц приблизительно на 15 дБ относительно друг друга. Требуемая величина максимальной девиации несущей частоты 50 кГц (для отечественного стандарта, и 75 кГц для западного) получается при изменении напряжения звуковой частоты на базе транзистора VT2, приблизительно равном 10—100 мВ. При больших величинах возможно появление искажений звука в виде хрипа (из-за нелинейности модуляционной характеристики или перегрузки входных каскадов УНЧ радиоприемника) и возникновение паразитной амплитудной модуляции.

В автогенераторах подобного типа ЧМ чаще всего основываются на изменении параметров колебательного контура или изменении потенциалов выводов генерирующего элемента. В данном случае применяется второй вид ЧМ, т. к. управляющее напряжение приложено к базе транзистора VT2, изменяя тем самым напряжение смещения на переходе база-эмиттер, и, соответственно, емкость цепи Б-3, которая является составной частью колебательного контура генератора. Данный контур включает в себя также катушку индуктивности L3, расположенную по ВЧ между базой и массой, и конденсаторы C13—C15. Конденсатор C15 включен в цепь обратной связи емкостной «трехточки», являясь одним из плеч делителя $C_{б\text{-}э}$ —C15, с которого снимается напряжение ОС. Емкость C15 позволяет регулировать уровень возбуждения и должна составлять примерно 5—8 пФ.

Для установки **оптимального режима работы генератора** и получения максимально возможной мощности необходимо правильно выбрать генерирующий элемент. При этом надо учитывать, что его верхняя граничная частота должна не менее чем в 5—6 раз превышать рабочую частоту передатчика. Этому требованию наиболее полно удовлетворяют транзисторы типа КТ355А, КТ372А-В, КТ326, КТ363А, Б. Хотя можно использовать и более распространенные — КТ315, КТ339 и др.

Совет.

Применение транзисторов структуры n-p-n более желательно, т. к. они обладают лучшей температурной стабильностью.

В генераторе необходимо исключить возможность появления сильной ПАМ. Ослабить ее можно правильным подбором рабочей точки генератора, зависящей от сопротивлений R7—R9. Резисторы R7 и R8 зашунтированы по ВЧ конденсаторами C10 и C11.

Величина сопротивления в цепи эмиттера составляет примерно 68—100 Ом, поэтому во избежание его влияния на колебательный контур, которое может вызвать чрезмерное расширение полосы частот резонансной кривой, последовательно с R9 включен дроссель L5, блокирующий прохождение токов ВЧ.

Раньше существовал специально выделенный для радиомикрофонов диапазон частот 57,5—58,5 МГц. Но в данной конструкции частота генерации передатчика находится в пределах 70—73 МГц, что позволяет использовать в качестве приемного устройства практически любой промышленный радиоприемник с отечественным УКВ диапазоном.

Это интересно знать.

Так поступают и за рубежом при производстве бытовых маломощных радиомикрофонов и средств радиоохранной сигнализации. Например, частота настройки японского радиомикрофона «Orion» равна 100 МГц и может перестраиваться в пределах 8 МГц (японо-американский широковещательный диапазон FM — 88...108 МГц).

Чтобы избежать возможных помех радиовещательным станциям и, наоборот, помех с их стороны, необходимо выбрать свободный участок УКВ диапазона. При этом смещение частоты радиомикрофона от ближайшей радиостанции должно быть не менее 250 кГц.

Можно перевести работу передатчика на второй радиовещательный диапазон УКВ 100—108 МГц.

Дроссели L1 и L2 индуктивностью 5—20 мкГн, резистор R1 и конденсаторы C1, C7 служат для развязки каскадов РМ по НЧ и ВЧ.

При напряжении питания 9 В потребляемый радиомикрофоном ток составляет около 20 мА, а мощность излучения при правильном согласовании с антенным контуром равна 5 мВт.

Данная схема без существенных переделок может работать на частотах до 120—150 МГц. При этом потребуется изменить лишь параметры колебательного контура.

Питание схемы. При определенных изменениях в номиналах некоторых резисторов и конденсаторов радиомикрофон может сохранять работоспособность при напряжении питания от 1,5 до 25 В. Для пита-

ния, в зависимости от конкретного применения, можно использовать различные источники напряжения, например, батарею типа «Корунд» или «Крона», аккумулятор 7Д-0,1. сетевые блоки питания должны иметь низкий уровень пульсаций выпрямленного напряжения (не более 10—20 мВ).

Радиомикрофон **монтируется** на печатной плате из одностороннего фольгированного стеклотекстолита толщиной 1—1,5 мм. При проектировании печатной платы и монтаже надо стремиться к тому, чтобы в схеме было как можно меньше нежелательных обратных связей, возникающих, в основном, из-за различных паразитных емкостей. Для этого длина выводов деталей и печатных дорожек должна быть минимальной, не следует делать печатные дорожки слишком широкими. Особенно это касается дорожек и выводов, примыкающих к базе и эмиттеру генерирующего транзистора. Каскады радиомикрофона удобнее всего располагать в линейку.

Связь колебательного контура с антенной — индуктивная. Но антенну можно также присоединить непосредственно к катушке колебательного контура L3 — ко второму (со стороны массы) витку через конденсатор емкостью 1—2 пФ. При этом длину антенны желательно уменьшить до 60—80 см во избежание внесения паразитной емкости в задающий контур и ухода в сторону частоты генерации. Для устранения микрофонного эффекта катушки L3 и L4 необходимо жестко закрепить на плате и после настройки залить парафином, эпоксидной смолой или закрепить клеем БФ2.

С целью снижения размеров конструкции и уменьшения паразитных емкостей следует использовать малогабаритные детали. Для сопротивлений подойдут резисторы типа ВС-0,25, МЛТ-0,125.

Переменные сопротивления — типа СПЗ-1, СПЗ-19, СПЗ-22А, СПЗ-38.

Необходимо особо остановиться на **подборе конденсаторов**, т. к. от них зависят многие параметры. В частотнозадающих цепях лучше всего использовать керамические конденсаторы типа КДУ, КД1 (корпус серого или голубого цвета), К10-17, К10-38, К26-1 с ТКЕ ПЗЗ, МПО или МЗЗ. В блокировочных цепях можно ставить К10У-5, К10-7В, К22У-1, К22-5, КМ-5.

Из подстроечных годятся КТ4-23, КПК-(М)Т, КПК-МН. На месте оксидных конденсаторов подойдут К50-16, К50-35, К50-38. Для изготовления контурных катушек L3 и L4 желательно применить посеребренный провод диаметром 1—2 мм.

Катушки безкаркасные с внутренним диаметром — 10 мм. Первая содержит 5, а вторая — 3 витка провода диаметром 1,5, индуктивностью L3=0,25 мкГн (для диапазона на 100—108 МГц — 4 и 2 витка соответственно, индуктивностью L3=0,19 мкГн).

При установке катушек L3 и L4 на плату следует иметь в виду, что расстояние между их центрами должно составлять примерно 8 мм.

В качестве **антенны** используется укороченный асимметричный диполь — четвертьволновый отрезок толстого многожильного провода длиной 80—100 см или подходящая телескопическая антенна (можно меньшей длины).

Индуктивность блокировочных дросселей L1 — L3 примерно равна 5—20 мкГц. Тип — Д(М)-1,2, ДПМ-0,1. Можно применить самодельные дроссели, намотав на корпусе резистора МЛТ-0,25 сопротивлением не менее 500 кОм 40—50 витков провода ПЭВ-0,1, уложенных в один ряд. Гнездо XSS1 — типа ГК2. Катушка 3L1 содержит 500 витков провода ПЭВ-0,1 на пермал-лоевом кольце.

Правильно собранная схема начинает работать сразу. О наличии генерации можно убедиться по изменению потребляемого тока при закорачивании на массу базы транзистора VT2 конденсатором емкостью порядка 0,01 мкФ.

Дальнейшая регулировка заключается в подборе рабочей точки транзистора VT2. При принудительном срыве генерации напряжение между базой и эмиттером VT2 должно быть около 0,66 В. Неустойчивость генерации при выходе генерирующего элемента из рабочего режима можно заметить по шумам, хрипам и резким изменениям звукового тона. Далее путем растяжения или сжатия витков катушки L3 необходимо подогнать частоту генератора под требуемое значение, которое должно выставляться при среднем положении ротора конденсатора C14.

При этом можно воспользоваться радиоприемником со шкалой принимаемых частот и индикатором уровня принимаемого сигнала, который пригодится при дальнейшей настройке. Для контроля настройки и качества модуляции на линейный вход радиомикрофона подается звуковой сигнал напряжением 0,2 В и частотой 1 кГц.

Точное значение частоты автогенератора подбирается вращением сердечника конденсатора C14 диэлектрической (пластмассовой) отверткой.

Совет.
При необходимости дальнейшей настройки следует помнить, что при несоответствии верхней границы диапазона регулировка производится подстроечным конденсатором, а нижней — изменением расстояния между витками катушки колебательного контура.

При налаживании необходимо учитывать, что от конденсаторов C13—C15 зависит частота генерации и девиация несущей (чувствительность модулятора по НЧ), C15 влияет на уровень возбуждения генератора. В заключение подстроечным конденсатором C12 необходимо настроить антенный контур L4C12 в резонанс с частотой передатчика и подобрать связь между катушками L3 и L4 по максимальной отдаваемой мощности.

Контроль настройки при этом ведется при помощи ВЧ вольтметра или индикатора уровня принимаемого сигнала.

Совет.
Особое внимание уделите уменьшению гармоник в выходном радиосигнале и не допускать эксплуатации радиомикрофона при значительном их уровне.

Устройство не должно создавать помех на частотах близлежащего диапазона. При $F_{ген}$, лежащей в диапазоне 66—73 МГц, можно проверить уровень третьей гармоники по помехам на 9—11 каналах телевизионного приемника. По этим же телеканалам можно проверить уровень второй гармоники диапазона 100—108 МГц.

Налаживать следует таким образом, чтобы гармоники не создавали каких-либо значительных помех на указанных частотах, помня о том, что они, как и ПАМ, во многом зависят от режима работы автогенератора.

Настройка микрофонного усилителя сводится:

- к подбору рабочего режима транзистора VT1 при помощи резисторов R2 и R3, определяющих напряжение смещения на базе VT1;
- установлению коэффициента усиления не менее 50 (при этом может потребоваться изменить сопротивление коллекторной нагрузки резистора R4).

При подаче на базу VT1 напряжения 2 мВ частотой 1 кГц переменное напряжение на коллекторе должно быть не менее 100 мВ. Уровень усиления можно контролировать, подключив на выход В микрофонного усилителя телефонный капсюль типа ТМ-4.

Используя данный передатчик, можно изготовить переговорное устройство с симплексной связью. **Симплексной** называется такая связь, при которой передача и прием ведутся поочередно: сначала одна радиостанция только передает, а другая только принимает, затем наоборот. Подробности см. на http://www.irls.narod.ru/«Каталог радиолюбительских схем».

Передатчик с микрофоном в контуре ВЧ генератора

Рассмотрим **передатчик с микрофоном в контуре ВЧ генератора,** размещенный на http://www.warning.dp.ua/tel2.htm. Значительно упростить конструкцию радиомикрофона можно при использовании малогабаритных конденсаторных микрофонов, включаемых непосредственно в колебательный контур высокочастотного генератора. Возможная схема такого передатчика представлена на **рис. 6.26.**

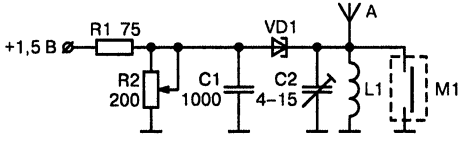


***Рис. 6.26.** Передатчик с микрофоном в контуре ВЧ генератора*

Конденсаторный микрофон выполнен в виде развернутого конденсатора с двумя плоскими неподвижными электродами. Параллельно электродам закреплена мембрана (тонкая фольга, металлизированная диэлектрическая пленка и т. п.). Она электрически изолирована от неподвижных электродов.

Выступая элементом контура, конденсаторный микрофон осуществляет частотную модуляцию. В остальном описание схемы и настройка передатчика аналогичны вышеприведенной схеме.

Мощность излучения вышеприведенных устройств, составляет доля единиц миливатт. Соответственно, и радиус действия этих устройств составляет единицы — десятки метров.

Микропередатчик с частотной модуляцией на биполярном транзисторе

Принципиальная схема микропередатчика с ЧМ на транзисторе (www.shema.org.ua) показана на **рис. 6.27.**

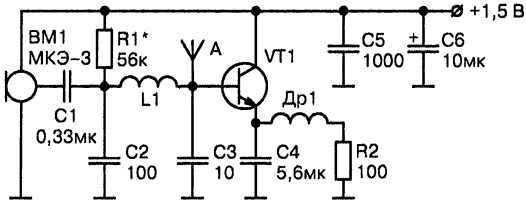


Рис. 6.27. *Микропередатчик с ЧМ на транзисторе*

Модулирующее напряжение, снимаемое с электретного микрофона МКЭ-3 (МКЭ-333, МКЭ-389, М1-А2 «Сосна»), через конденсатор С1 поступает на базу транзистора VT1, на котором выполнен задающий генератор.

Управляющее напряжение приложено к базе транзистора VT1. Поэтому, изменяя напряжение смещения на переходе база-эмиттер, и, соответственно, емкость цепи база-эмиттер, которая является одной из составных частей колебательного контура задающего генератора, осуществляется частотная модуляция передатчика.

Этот контур включает в себя также катушку индуктивности L1, расположенную по высокой частоте между базой транзистора VT1 и массой, и конденсаторами С3 и С4. Конденсатор С4 включен в цепь обратной связи емкостной трехточки, являясь одним из плеч делителя С6—С4, с которого и снимается напряжение обратной связи.

Емкость конденсатора С4 позволяет регулировать уровень возбуждения. Нужно избежать влияния шунтирующего резистора R2 в цепи эмиттера транзистора VT1 на колебательный контур. Ведь оно может вызвать чрезмерное расширение полосы частот резонансной кривой. Поэтому последовательно с резистором R2 включен дроссель Др1, блокирующий прохождение токов высокой частоты. Индуктивность этого дросселя должна иметь величину около 20 мкГн. Катушка L1 — бескаркасная, диаметром 3 мм намотана проводом ПЭВ 0,35 и содержит 7-8 витков.

Для получения максимально возможной мощности необходимо правильно выбрать генерирующий элемент (транзистор VT1) и установить оптимальный режим работы генератора. Для этого необходимо применять транзисторы, верхняя граничная частота которых должна превышать рабочую частоту генератора не менее чем в 7-8 раз. Этому условию наиболее полно отвечают транзисторы типа n-p-n КТ368, хотя можно использовать и более распространенные транзисторы КТ315 или КТ3102.

Миниатюрный радиопередатчик на одном биполярном транзисторе с питанием от батареи для электронных часов

Миниатюрный радиопередатчик с питанием от батареи для электронных часов рассмотрен на http://cxem.net/radiomic/radiomic53.php. Схема радиопередатчика приведена на **рис. 6.28.**

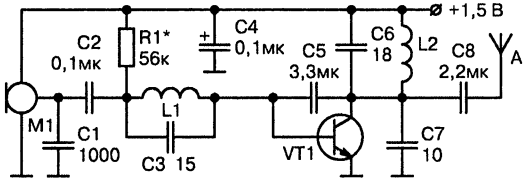


Рис. 6.28. *Миниатюрный радиопередатчик с питанием от батареи для электронных часов*

Устройство содержит минимум необходимых деталей и питается от батарейки для электронных часов напряжением 1,5 В. При столь малом напряжении питания и потребляемом токе 2—3 мА сигнал этого радиомикрофона может приниматься на удалении до 150 м. Продолжительность работы около 24 ч.

Задающий генератор собран на транзисторе VT1 типа КТ368, режим работы которого по постоянному току задается резистором R1. Частота колебаний задается контуром в базовой цепи транзистора VT1. Этот контур включает в себя катушку L1, конденсатор C3 и емкость цепи база-эмиттер транзистора VT1. В коллекторную цепь транзистора VT1 в качестве нагрузки включен контур, состоящий из катушки L2 и конденсаторов C6, C7.

Конденсатор C5 включен в цепь обратной связи и позволяет регулировать уровень возбуждения генератора.

Это интересно знать.
В автогенераторах подобного типа частотная модуляция производится путем изменения потенциалов выводов генерирующего элемента.

В нашем случае управляющее напряжение прикладывается к базе транзистора VT1, изменяя тем самым напряжение смещения на переходе база-эмиттер и, как следствие, изменяя емкость перехода база-эмиттер. Изменение этой емкости приводит к изменению резонанс-

ной частоты колебательного контура, что и приводит к появлению частотной модуляции.

Это интересно знать.

При использовании УКВ импортного приемника требуемая величина максимальной девиации несущей частоты составляет 75 кГц (для отечественного стандарта — 50 кГц) и получается при изменении напряжения звуковой частоты на базе транзистора в диапазоне 10—100 мВ.

Именно поэтому в данной конструкции не используется модулирующий усилитель звуковой частоты. При использовании электретного микрофона с усилителем, например, МКЭ-3, М1-Б2 «Сосна», уровня сигнала, снимаемого непосредственно с выхода микрофона, оказалось достаточно для получения требуемой девиации частоты радиомикрофона.

Конденсатор С1 осуществляет фильтрацию колебаний высокой частоты. Конденсатором С7 можно в небольших пределах изменять значение несущей частоты.

Сигнал в антенну поступает через конденсатор С8, емкость которого специально выбрана малой для уменьшения влияния возмущающих факторов на частоту колебаний генератора. Антенна сделана из провода или металлического прутка длинной 60—100 см. Длину антенны можно уменьшить, если между ней и конденсатором С8 включить удлинительную катушку L3.

Катушки радиомикрофона бескаркасные, диаметром 2,5 мм, намотаны виток к витку. Катушка L1 имеет 8 витков, катушка L2 — 6 витков, катушка L3 — 15 витков провода ПЭВ 0,3. При настройке устройства добиваются получения максимального сигнала высокой частоты, изменяя индуктивности катушек L1 и L2. Подбором конденсатора С7 можно немного изменять величину несущей частоты, в некоторых случаях его можно исключить совсем.

Радиопередатчик с частотной модуляцией и рабочим диапазоном частот 61—73 МГц

Радиопередатчик с ЧМ в УКВ диапазоне частот 61—73 МГц приведен на http://cxem.net/radiomic/radiomic27.php. Радиопередатчик (**рис. 6.29**) представляет собой однокаскадный УКВ ЧМ передатчик,

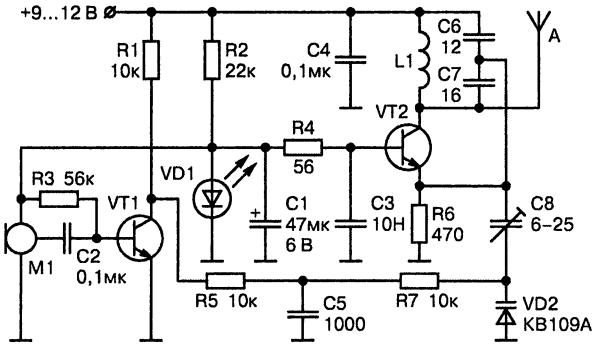


Рис. 6.29. *Радиопередатчик с ЧМ в УКВ диапазоне частот 61—73 МГц*

работающий в вещательном диапазоне 61—73 МГц. Выходная мощность передатчика при использовании источника питания с напряжением 9—12 В составляет примерно 20 мВт. Он обеспечивает дальность передачи информации около 150 м при использовании приемника с чувствительностью 10 мкВ.

Режимы транзисторов УЗЧ (VT1) и генератора ВЧ (VT2) по постоянному току задаются резисторами R3 и R4, соответственно. Напряжение 1,2 В на них и микрофон M1 подается с параметрического стабилизатора на R1, C1, VD1.

Это интересно знать.

Поэтому устройство сохраняет свою работоспособность при снижении напряжения питания до 4—5 В. При этом наблюдается уменьшение выходной мощности устройства, а несущая частота изменяется незначительно.

Модулирующий усилитель выполнен на транзисторе VT1 типа КТ315. Напряжение звуковой частоты на его вход поступает с электретного микрофона с усилителем M1 типа МКЭ-3 и ему подобным. Усиленное напряжение звуковой частоты с коллектора транзистора VT1 поступает на варикап VD2 типа КВ109А через фильтр нижних частот на резистор R5 и конденсатор C5, а также резистор R7.

Варикап VD1 включен последовательно с подстроечным конденсатором C8 в эмнттерную цепь транзистора VT2. Частота колебаний задающего генератора, выполненного на транзисторе VT2 типа КТ315 (КТ3102, КТ368), определяется элементами контура L1, C6, C7 и емкостью C8 и VD1.

Вместо светодиода VD1 типа АЛ307 можно использовать любой другой светодиод или три последовательно включенных в прямом направлении диода типа КД522 и им подобных.

Катушка L1 бескаркасная, диаметром 8 мм, имеет 6 витков провода ПЭВ 0,8.

Наладка. При налаживании передатчик настраивают на свободный участок УКВ ЧМ диапазона сжатием или растяжением витков катушки L1 или подстройкой конденсатора С8. Девиация частоты устанавливается конденсатором С8 по наиболее качественному приему на контрольный приемник.

Передатчик можно настроить и на вещательный диапазон FM (88—108 МГц), для этого необходимо уменьшить число витков L1 до 5 и емкость конденсаторов С6 и С7 до 10 пФ. В качестве антенны используется отрезок провода длинной 60 см. Для уменьшения влияния дестабилизирующих факторов антенну можно подключить через конденсатор емкостью 1—2 пФ.

Радиопередатчик с амплитудной модуляцией и рабочим диапазоном частот 27—28 МГц

Радиопередатчик с АМ в диапазоне частот 27—28 МГц приводится на http://www.warning.dp.ua/tel21.htm. Он представляет собой передатчик, работающий в диапазоне 27—28 МГц с амплитудной модуляцией. Дальность действия до 100 м (**рис. 6.30**).

Передатчик состоит из генератора высокой частоты, собранного на транзисторе VT2 типа КТ315, и однокаскадного усилителя звуковой частоты на транзисторе VT1 типа КТ315. На вход последнего через конденсатор С1 поступает звуковой сигнал от микрофона М1 типа «Сосна».

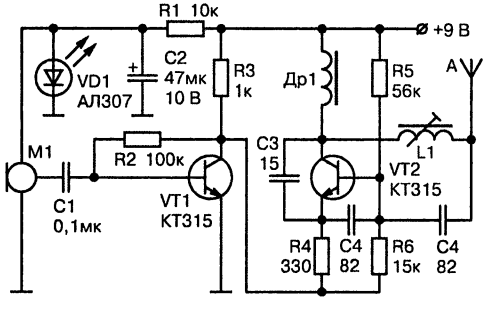


Рис. 6.30. Радиопередатчик с АМ в диапазоне частот 27—28 МГц

Нагрузку усилителя составляют:

- резистор R3;
- генератор высокой частоты, включенный между плюсом источника питания и коллектором транзистора VTI.

С усилением сигнала напряжение на коллекторе транзистора VT1 изменяется. Этим сигналом и модулируется амплитуда сигнала несущей частоты генератора передатчика, излучаемая антенной.

Детали. В конструкции использованы резисторы МЛТ-0,125, конденсаторы — К10-7В. Вместо транзисторов КТ315 можно использовать КТ3102.

Катушка L1 намотана на каркасе из полистирола диаметром 7 мм. Она имеет подстроечный сердечник из феррита 600НН диаметром 2,8 мм и длиной 12 мм. Катушка L1 содержит 8 витков провода ПЭВ 0,15 мм. Намотка — виток к витку.

Дроссель Др1 намотан на резисторе МТЛ-0,5 сопротивлением более 100 кОм. Обмотка дросселя содержит 80 витков ПЭВ 0,1. В качестве антенны используется стальной упругий провод длиной 20 см.

При **настройке** частоту устанавливают подстройкой индуктивности катушки L1. После регулировки подстроечный сердечник катушки закрепляется парафином.

Радиопередатчик с широкополосной частотной модуляцией и рабочим диапазоном частот 65—108 МГц

Радиопередатчик с широкополосной ЧМ в диапазоне частот 65—108 МГц рассматривается на http://www.radiomaster.net/load/17-45/index.html. Схема радиопередатчика представлена на **рис. 6.31.**

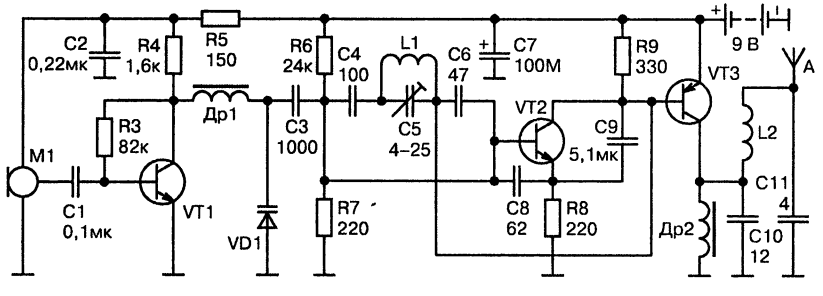


Рис. 6.31. Радиопередатчик с широкополосной ЧМ в диапазоне частот 65—108 МГц

Радиомикрофон позволяет принимать сигнал на обычный ЧМ приемник этого диапазона. Дальность действия достигает 150—200 м. Продолжительность работы с батареей типа «КРОНА» — около 10 ч.

Низкочастотные колебания с выхода микрофона М1 (типа МКЭ-3, М1-Б2 «Сосна» и им подобных) через конденсатор С1 поступают на усилитель звуковой частоты, выполненный на транзисторе VT1 типа КТ315. Усиленный сигнал звуковой частоты, снимаемый с коллектора транзистора VT1, через дроссель Др1 воздействует на варикап VD1 (типа КВ109А), который осуществляет частотную модуляцию радиосигнала, сформированного высокочастотным генератором.

Генератор ВЧ собран на транзисторе VT2 типа КТ315. Частота этого генератора зависит от параметров контура L1, С3, С4, С5, С6, VD1. Сигнал ВЧ, снимаемый с коллектора транзистора VT2, усиливается усилителем мощности на транзисторе VT3 типа КТ361. Усилитель мощности имеет гальваническую связь с задающим генератором.

Усиленное высокочастотное напряжение выделяется на дросселе Др2 и поступает на П-образный контур, выполненный на элементах С11, L2, С10. Последний настроен на пропускание основного сигнала и подавление множества гармоник, возникающих на коллекторе транзистора VT3.

Радиомикрофон собран на плате размером 30×70 мм.

В качестве **антенны** используется отрезок монтажного провода длиной 25 см.

Детали. Все детали малогабаритные. Резисторы — типа МЛТ-0,125, конденсаторы — К50-35, КМ, КД. Вместо варикапа VD1 типа КВ109А можно использовать варикапы с другим буквенным индексом иди варикап типа КВ102. Транзисторы могут иметь любой буквенный индекс.

Транзисторы VT1 и VT2 можно заменить на КТ3102, КТ368, а транзистор VT3 — на КТ326, КТ3107. Дроссели Др1 и Др2 намотаны на резисторах МЛТ-0,25 сопротивлением более 100 кОм проводом ПЭВ 0,1 по 60 витков каждый. Катушки L1 и L2 бескаркасные, диаметром 5 мм. Катушка L1 — 3 витка, катушка L2 — 13 витков провода ПЭВ 0,3.

Настройка сводится к установке частоты задающего генератора, соответствующей свободному участку УКВ ЧМ диапазона, изменением емкости подстроечного конденсатора. Передатчик настраива-

ется на максимальную мощность ВЧ сигнала растяжением или сжатием витков катушки L2.

Радиопередатчик средней мощности с компактной рамочной антенной

Радиопередатчик средней мощности с компактной рамочной антенной приводится на http://www.radiomaster.net/load/17-45/index.html. Устройство работает в диапазоне 65—73 МГц с частотной модуляцией. Дальность действия при использовании рамочной компактной антенны составляет около 150 м. Продолжительность работы устройства при использовании батареек «Крона» составляет 30 ч. Принципиальная схема радиопередатчика представлена на **рис. 6.32.**

Низкочастотный сигнал микрофона М1 типа МКЭ-3, «Сосна» и др. усиливается двухкаскадным усилителем низкой частоты с непосредственными связями. Усилитель выполнен на транзисторах VT1 и VT2 типа КТ315. Режим работы усилителя устанавливается резистором R2.

Задающий генератор устройства выполнен на транзисторе VT3 типа КТ315. Частотозадающий контур подключается к базе транзистора VT3 через конденсатор С6 небольшой емкости. Конденсаторы С8, С9 образуют цепь обратной связи. Контур генератора состоит из индуктивности L1, конденсатора С5 и двух, включенных встречно, диодов типа КД102.

Под действием модулирующего напряжения емкости диодов VD1, VK2 изменяются. Таким образом, осуществляется частотная модуляция передатчика. С выхода генератора модулированный сигнал пода-

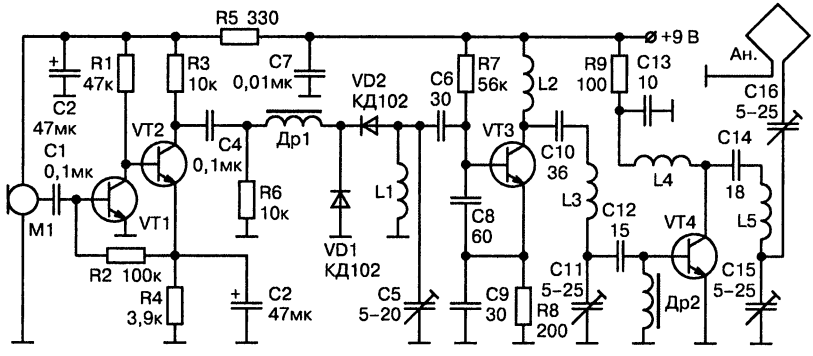


Рис. 6.32. *Радиопередатчик средней мощности с компактной рамочной антенной*

ется на усилитель мощности. Выходной усилитель выполнен на транзисторе VT4 типа КТ315. Он работает с высоким КПД в режиме класса «С». Усиленный сигнал поступает в рамочную антенну, выполненную в виде спирали. Спираль может быть любой формы, важно только, чтобы общая длина провода составляла 85—100 см, диаметр провода 1 мм.

Детали. Дроссели Др1, Др2 — любые, с индуктивностью около 30 мкГн. Катушки L1, L2, L3, L4, L5 — бескаркасные, диаметром 10 мм. Катушка L1 имеет 7 витков, L2 и L4 — по 4 витка, L3 и L5 — по 9 витков. Все катушки намотаны проводом ПЭВ 0,8 мм. Настройка передатчика особенностей не имеет.

Миниатюрный ЧМ радиопередатчик УКВ диапазона на дискретных элементах с дальностью действия 300 м

ЧМ радиопередатчик УКВ диапазона с дальностью действия 300 м представлена на http://www.radiomaster.net/load/17-45/index.html. Этот передатчик при весьма малых размерах позволяет передавать информацию на расстоянии до 300 м. Прием сигнала может вестись на любой приемник ЧМ УКВ диапазона. Для питания может быть использован любой источник питания с напряжением 5—15 В. Схема передатчика приведена на **рис. 6.33**.

Задающий генератор передатчика выполнен на полевом транзисторе VT2 типа КП303. Частота генерации определяется элементами L1, C5, C3, VD2. Частотная модуляция осуществляется путем подачи модулирующего напряжения звуковой частоты на варикап VD2 типа

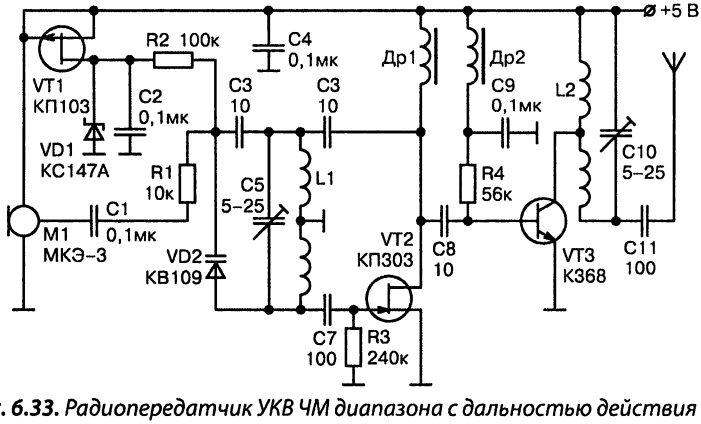


Рис. 6.33. *Радиопередатчик УКВ ЧМ диапазона с дальностью действия 300 м*

КВ109. Рабочая точка варикапа задается напряжением, поступающим через резистор R2 со стабилизатора напряжения.

Стабилизатор включает в себя генератор стабильного тока на полевом транзисторе VT1 типа КП103, стабилитрон VD1 типа КС147А и конденсатор С2.

Усилитель мощности выполнен на транзисторе VT3 типа КТ368. Режим работы усилителя задается резистором R4. В качестве антенны используется отрезок провода длиной 15—50 см.

Детали. Дроссели Др1 и Др2 могут быть любые, с индуктивностью 10—150 мГн. Катушки L1 и L2 наматываются на полистироловых каркасах диаметром 5 мм с подстроечными сердечниками 100 ВЧ или 50 ВЧ. Количество витков — 3,5 с отводом от середины, шаг намотки 1 мм, провод ПЭВ 0,5 мм. Вместо транзистора КП303 можно использовать КП302, КП307.

Настройка заключается в установке необходимой частоты генератора конденсатором С5, получения максимальной выходной мощности путем подбора сопротивления резистора R4 и подстройке резонансной частоты контура конденсатором С10.

Мощный высокочастотный радиопередатчик с частотной модуляцией и с рабочим диапазоном частот 65—108 МГц

Мощный высокочастотный радиопередатчик с ЧМ в диапазоне частот 65—108 МГц рассмотрен на http://pk.altnet.ru/index.php?id=3-9. Это устройство (**рис. 6.34**) работает в диапазоне 65—108 МГц с частотной модуляцией. Дальность действия составляет около 100 м при использовании компактной антенны. При использовании штыревой антенны дальность может достигать 500—600 м.

Сигнал от электретного микрофона М1 типа МКЭ-3 поступает на двухкаскадный низкочастотный усилитель с непосредственными связями на транзисторах VT1, VT2 типа КТ315. Рабочая точка усилителя устанавливается автоматически цепью обратной связи по постоянному току через R5, R6, С3. Усиленный низкочастотный сигнал с коллектора транзистора VT2 через фильтр низкой частоты на элементах R9, С4 и резистор R10 поступает на варикап VD1 типа КВ109, включенный в эмиттерную цепь транзистора VT3 типа КТ904.

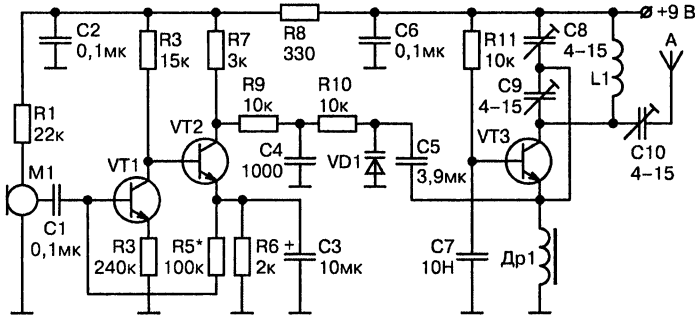


Рис. 6.34. *Мощный высокочастотный радиопередатчик с ЧМ в диапазоне частот 65—108 МГц*

Напряжение смещения на варикап VD1 задается коллекторным напряжением транзистора VT2. Однокаскадный ВЧ генератор выполнен на транзисторе VT3. Напряжение смещения на базе этого транзистора задается резистором R11. Транзистор VT3 включен по схеме с общей базой. В его коллекторной цепи включен контур C8, C9, L1.

Частота настройки генератора определяется индуктивностью катушки L1 и емкостями C8, C5, VD1. Конденсатор C9 устанавливает глубину обратной связи, а конденсатор C10 согласует контур с антенной.

Детали. Все детали передатчика малогабаритные. Дроссель Др1 типа ДПМ 0,1 на 60 мкГн. Его можно заменить на самодельный, намотанный на резисторе МЛТ-0,25 сопротивлением более 100 кОм проводом ПЭВ 0,1 100 витков.

Катушка L1 — бескаркасная, с внутренним диаметром 8 мм, имеет 7 витков провода ПЭВ 0,8 мм. Компактная катушечная антенна выполнена тем же проводом, ее общая длина составляет 50 см. Катушка имеет диаметр 3 см. Если используется обычная антенна, то это провод или штырь длиной 0,75—1,0 м.

Настройка. При настройке конденсатором C8 настраивают радиомикрофон на свободный участок УКВ ЧМ диапазона. Конденсаторами C9 и C10 настраивают генератор на максимальную дальность связи. Мощность передатчика составляет около 200 мВт.

Если такая мощность не нужна, то ее легко понизить, увеличив вместе с тем срок службы источника питания. Для этого нужно увеличить сопротивление резистора R11 до 68—100 кОм и заменить дроссель Др1 на постоянный резистор сопротивлением 180—330 Ом. Так

как в этом случае мощность радиомикрофона будет около 10 мВт, то транзистор VT3 можно заменить на КТ315 или КТ3102.

Транзисторы VT1, VT2 могут быть заменены на КТ3102, а транзистор VT3 — на КТ606, КТ907.

Для питания устройства используется батарея на 9 В типа «Крона», «Корунд» или аккумулятор 7Д-0,15.

Радиопередатчик с узкополосной частотной модуляцией и с рабочим диапазоном частот 140—150 МГц

Радиопередатчик с узкополосной ЧМ в диапазоне частот 140—150 МГц (http://vrtp.ru/index.php?s). Схема радиопередатчика представлена на **рис. 6.35**. Он работает в диапазоне 140—150 МГц с узкополосной частотной модуляцией. Девиация частоты — 3 кГц. Частота задающего генератора стабилизирована кварцевым резонатором. В качестве акустического преобразователя используется электретный микрофон М1 с усилителем типа МКЭ-3, «Сосна», МЭК-1, и др.

Питание на микрофон поступает через RC-фильтр, состоящий из резистора R1 и конденсатора C1. Напряжение звуковой частоты с выхода микрофона М1 через разделительный конденсатор C2 поступает на вход усилителя звуковой частоты (база транзистора VT1).

Усилитель звуковой частоты собран по двухкаскадной схеме с активными элементами на транзисторах VT1 и VT2 типа КТ315. Он усиливает и ограничивает звуковой сигнал до необходимой амплитуды. Режимы работы транзисторов VT1, VT2 по постоянному току устанавливаются путем подбора сопротивления резистора R3.

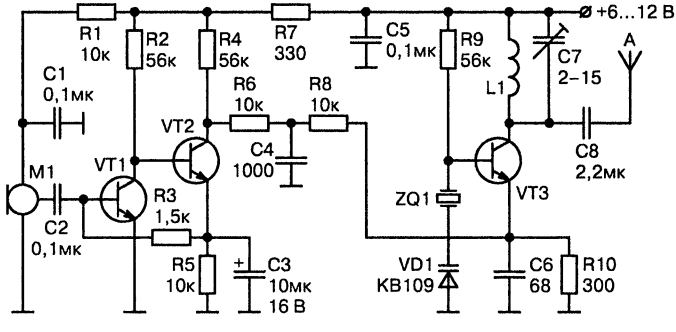


Рис. 6.35. Радиопередатчик с узкополосной ЧМ в диапазоне частот 140—150 МГц

Это интересно знать.
Заданный режим поддерживается далее автоматически с помощью обратной связи между транзисторами VT1 и VT2.

Усиленный и ограниченный сигнал звуковой частоты через RC-фильтр низкой частоты, выполненный на резисторах R6, R8 и конденсаторе C4, поступает на варикап VD1 типа КВ109. Под действием переменного напряжения изменяется емкость варикапа VD1, осуществляя тем самым частотную модуляцию.

Постоянное напряжение, снимаемое с коллектора транзистора VT2, задает начальное смещение на варикапе VD1. Задающий генератор выполнен на транзисторе VT3 типа КТ368, КТ3101. Режим транзистора VT3 по постоянному току определяет резистор R9 в его базовой цепи. Кварцевый резонатор ZQ1 используется на частоту 47—49 МГц.

Контур в коллекторной цепи транзистора VT3 настроен на частоту третьей гармоники используемого кварцевого резонатора. Высокочастотный сигнал поступает в антенну через конденсатор малой емкости C8.

В качестве **антенны** используется отрезок провода длинной 40—50 см.

Катушка L1 наматывается проводом ПЭВ 0,6 мм на корпусе подстроечного конденсатора C7 и содержит 3—4 витка. Выводы катушки припаиваются к выводам конденсатора.

Настройка усилителя звуковой частоты заключается в подборе сопротивления резистора R3 так, чтобы получить на коллекторе транзистора VT2 напряжение, равное примерно половине напряжения источника питания. Контур L1, C7 настраивается по максимуму излучаемой мощности путем подстройки конденсатора C7.

Радиопередатчик с высокой стабильностью несущей частоты и с рабочим диапазоном 61—74 МГц

Радиопередатчик с высокой стабильностью несущей частоты рассматривается на http://cxem.net/radiomic/radiomic30.php.

При использовании кварцевого резонатора с высокой частотой появляется возможность создать простой радиомикрофон с высокой стабильностью несущей частоты. Ниже приведено описание подобного устройства. Радиомикрофон работает в диапазоне 61—74 МГц с частотной модуляцией.

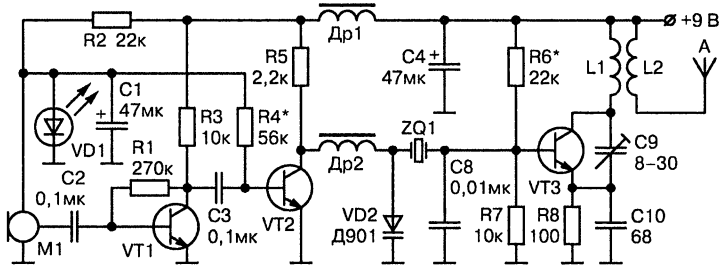


Рис. 6.36. Радиопередатчик с высокой стабильностью несущей частоты

Принципиальная схема передатчика радиопередатчика приведена на **рис. 6.36**.

Сигнал с микрофона M1 типа МКЭ-3 усиливается двухкаскадным усилителем на транзисторах VT1, VT2 типа КТ315. Задающий генератор выполнен на транзисторе VT3 типа КТ368. Частотная модуляция несущей частоты обеспечивается варикапом VD2. Резисторы R6 и R7 в базовой цепи транзистора VT3 определяют его режим по постоянному току.

Конденсатор C9 устанавливает необходимый режим генерации, обеспечивая положительную обратную связь. Стабильность частоты генератора зависит в основном от напряжения питания. Чтобы ее повысить, необходимо использовать стабилизатор на 6—9 В, что приведет к усложнению схемы.

Стабилизировать частоту можно и другим способом. Если быть точным, то причина нестабильности несущей частоты определяется в основном колебаниями рабочей точки транзистора VT2 усилителя звуковой частоты при изменении напряжения питания.

Положение этой рабочей точки определяет напряжение обратного смещения на варикапе VD2, а значит, и его начальную емкость. Для стабилизации рабочей точки усилителя на транзисторе VT2 в его базовую цепь включен резистор R4, напряжение на который поступает с параметрического стабилизатора, собранного на резисторе R2, светодиоде VD1 и конденсаторе C1. В устройстве использованы постоянные резисторы МЛТ-0,125, конденсаторы типов К50-16 и КМ.

Детали. Дроссели Др1, Др2 можно использовать стандартные, например, типа Д-0,1, с индуктивностью 15—30 мкГн или изготовить самостоятельно. Дроссели наматываются на резисторах МЛТ-0,25 сопротивлением более 100 кОм и содержат 50—60 витков провода

ПЭВ 0,1 мм. Контурная катушка L1 намотана на каркасе диаметром 8 мм и содержит 6 витков провода ПЭВ 0,8 мм.

Катушка L2 намотана на том же каркасе и тем же проводом, что и катушка L1. Катушка L2 содержит 3 витка, размещенных на расстоянии 1 мм от витков катушки L1.

Антенна выполнена следующим образом: отрезок 50-омного кабеля длиной 10—12 см зачищается от изоляции и удаляется центральная жила. По всей длине отрезка кабеля наматывается виток к витку провод ПЭВ-0,6 — антенна готова. В крайнем случае, в качестве антенны можно использовать провод длиной 30—50 см.

Настройку начинают с усилителя звуковой частоты. Изменением сопротивления резистора R4 устанавливают напряжение на коллекторе транзистора VT2, равное половине напряжения источника питания. Емкость конденсатора C9 необходимо подобрать по максимуму тока, потребляемому генератором, а затем резистором R6 установить этот ток около 10 мА.

Радиопередатчик повышенной мощности без дополнительного усилителя мощности и с рабочим диапазоном частот 27—28 МГц

Радиопередатчик повышенной мощности без дополнительного усилителя мощности рассмотрен на http://cxem.net/radiomic/radiomic43.php. От предыдущих устройств предлагаемый радиопередатчик отличается конструкцией задающего генератора, позволяющей получить повышенную мощность излучения без использования дополнительного усилителя мощности.

Схема устройства показана на **рис. 6.37.**

Радиопередатчик работает на частоте 27—28 МГц с амплитудной модуляцией. Частота несущей стабилизирована кварцем, что позволяет увеличить дальность связи при использовании приемника с кварцевой стабилизацией частоты.

Питается устройство от источника питания напряжением 3—4,5 В. Усилитель звуковой частоты выполнен на транзисторе VT1 типа КТ315. Для питания микрофона и задания режимов по постоянному току транзисторов VTI, VT2, VT3 используется параметрический стабилизатор напряжения на резисторе R2, светодиоде VD1 и конденсаторе C1.

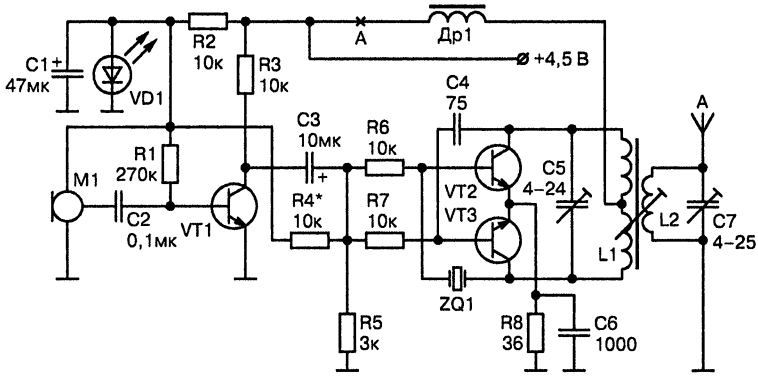


Рис. 6.37. *Радиопередатчик повышенной мощности без дополнительного усилителя мощности*

Напряжение 1,2 В поступает на электретный микрофон с усилителем M1 типа МКЭ-3, «Сосна» и др. Напряжение звуковой частоты с микрофона M1 через конденсатор C2 поступает на базу транзистора VT1. Режим работы этого транзистора по постоянному току задается резистором R1.

Усиленный сигнал звуковой частоты, снимаемый с коллекторной нагрузки транзистора VT1 — резистора R3, через конденсатор C3 поступает на задающий генератор, осуществляя тем самым амплитудную модуляцию передатчика.

Задающий генератор передатчика собран на двух транзисторах VT2 и VT3 типа КТ315 и представляет собой двухтактный автогенератор с кварцевой стабилизацией в цепи обратной связи.

Контур, состоящий из катушки L1 и конденсатора C5, настроен на частоту кварцевого резонатора ZQ1. Контур, состоящий из катушки L2 и конденсатора C7, предназначен для согласования антенны и передатчика.

Детали. В устройстве применены резисторы МЛТ-0,125. Конденсаторы использованы на напряжение более 6,3 В. Транзистор VT1 можно заменить на любой n-p-n транзистор, например, на КТ3102, КТ312. Транзисторы VT2, VT3 можно заменить на КТ3102, КТ368 с одинаковым коэффициентом передачи по току. Хороший результат можно получить при использовании микросхемы КР159НТ1, представляющей собой пару идентичных транзисторов.

Контурные катушки намотаны на каркасе диаметром 5 мм, имеющем подстроечный сердечник из карбонильного железа диаметром

3,5 мм. Намотка катушек ведется с шагом 1 мм. Катушка L1 имеет 4+4 витка, катушка L2 — 4 витка. Обе катушки намотаны проводом ПЭВ 0,5. Дроссель Др1 имеет индуктивность 20—50 мкГн. В качестве антенны используется провод длиной около 1 м.

В качестве **источника питания** можно использовать одну плоскую батарею КБС-4,5 В или четыре элемента типа А316, А336, А343.

Светодиод VD1 типа АЛ307 можно заменить любым другим.

Настройку передатчика начинают с установки режимов транзисторов VT2 и VT3 по постоянному току. Для этого подключают миллиамперметр в разрыв цепи питания в точке А и подбирают величину сопротивления резистора R4 такой, чтобы ток был равен 40 мА.

Настройку контуров L1, L2, C5, C7 проводят по максимуму ВЧ излучения. Причем грубо на рабочую частоту настраивают конденсаторами, а точнее — сердечником катушки. Подстроечник катушек L1, L2 должен находиться на расстоянии не более чем 3 мм от центра катушек, т. к. в крайних его положениях генерация может срываться из-за нарушения симметрии плеч транзисторов VT2, VT3.

Радиостетоскопы

Это полезно запомнить.

Радиостетоскопы *— контактные микрофоны, конструкционно объединенные с микропередатчиками, которые перехватывают акустические сигналы по виброакустическому (вибрационному) каналу утечки информации.*

В качестве чувствительных элементов в них обычно используются **пьезомикрофоны**, электретные микрофоны или датчики **акселерометрического** типа.

Питание акустических закладок осуществляется от автономных источников питания (аккумуляторов, батарей), электросети переменного тока, телефонной сети, а также от источников питания радиоэлектронной аппаратуры, в которой они устанавливаются.

В зависимости от мощности излучения и типа источника питания время работы акустической закладки составляет от нескольких часов до нескольких суток и даже месяцев. При электропитании от сети переменного тока или телефонной линии время работы не ограничено.

Это интересно знать.

Большинство радиозакладок с автономными источниками питания имеют мощность излучения до 10 мВт и дальность передачи информации до 100—200 м. Однако встречаются закладки с мощностью излучения в несколько десятков милливатт и дальностью передачи информации до 500—1000 м.

При использовании внешних источников питания (например, электросети или автомобильных аккумуляторов) мощность излучения может составлять более 100 мВт, что обеспечивает дальность передачи информации до несколько километров.

Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа «агентов» в выделенные помещения. Их датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

При этом возможности по перехвату информации будут во многом определяться затуханием информационного сигнала в ограждающих конструкциях и разборчивостью речи в месте установки контактного микрофона (**табл. 6.1, 6.2**).

Затухание вибрационных сигналов на ограждающих конструкциях *Таблица 6.1*

Наименование конструкции	Затухание сигнала, дБ
Стена в 0,5 кирпича	40 — 48
Стена в 1 кирпич	44—53
Стена в 2 кирпича	46—60
Стена из железобетонных блоков (100 мм)	40—50
Стена из железобетонных блоков (200 мм)	44—60
Окно одинарное (4 мм)	22—28
Окно двойное (4 мм)	32—48
Дверь типовая	23—34
Дверь металлическая, облицованная	32—48

Разборчивость речи при перехвате информации средствами разведки по прямому акустическому и виброакустическому каналам *Таблица 6.2*

Место установки датчика аппаратуры акустической разведки	Вид принимаемого сигнала	Словесная разборчивость, %
За окном на расстоянии 1,0—1,5 м от оконной рамы при закрытой форточке	Прямой акустический	67—80
За окном на расстоянии 1,0—1,5 м от оконной рамы при открытой форточке	Прямой акустический	97—98
На оконной раме или внешнем оконном стекле при закрытой форточке	Виброакустический	71—80
За дверью (без тамбура)	Прямой акустический	91—97
За перегородкой из материалов типа гипсолит, асбестоцемент	Прямой акустический	71—87
На перегородке из материалов типа гипсолит, асбестоцемент	Виброакустический	84—95
На железобетонной стене	Виброакустический	80—98
В воздуховоде (6—8 м от ввода)	Прямой акустический	87—95
На трубопроводе (через этаж)	Виброакустический	95—97

ОБНАРУЖИТЕЛИ РАДИОМИКРОФОНОВ: РАЗРАБОТКА, СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ

В последние годы подслушивание разговоров с помощью радиомикрофонов получило заметное распространение как в бизнесе, так и в быту. На радиорынках сегодня можно без труда приобрести различные «жучки» любой степени сложности. Обнаружить работающие радиомикрофоны можно с помощью приемников (сканеров), «просматривающих» электромагнитное излучение в широкой полосе частот — от килогерц до гигагерц.

Назначение индикаторов высокочастотного радиоизлучения

Профессиональные приемники обычно весьма дороги. Но на определенном уровне эту проблему удается решить и с помощью более простых устройств — сигнализаторов и индикаторов наличия высокочастотного поля.

Индикатор высокочастотного радиоизлучения является интересным и полезным прибором, с помощью которого удобно «осязать» состояние электронного изделия или помещения для обнаружения ВЧ излучений.

В этой главе описаны несложные устройства, позволяющие обнаруживать каналы утечки информации и демонстрирующие способы защиты от утечки информации, системы для предотвращения проникновения к охраняемому объекту, использующие различные физические принципы.

Представлены схемотехнические решения, как на доступных дискретных элементах, так и на специализированных микросхемах.

Простейший индикатор поля

Рассмотрим для начала простой идикатор поля, который представил на сайте http://cxem.net tolik777 (aka Viper). **Достоинством** схемы

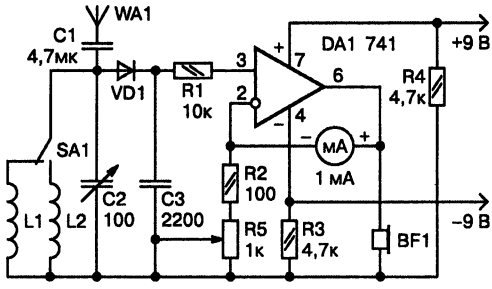


Рис. 7.1. Схема простого индикатора поля

является ее простота. Но этой схеме присущ очень большой **недостаток**, а именно низкая фильтрация на входе (**рис. 7.1**).

Это интересно знать.

*Из-за **низкой фильтрации на входе** индикатор реагирует даже на электрическую проводку в помещении, к тому же он имеет **очень низкую чувствительность** (порядка 50 мВ), поэтому маломощные передатчики находить затруднительно.*

Рассмотрим работу принципиальной схемы. Сигнал, принятый антенной WA, детектируется диодом VD1, а выделенный низкочастотный сигнал усиливается микросхемой DA1. Питание микросхемы однополярное. Коэффициент усиления регулируется переменным резистором R5. На выходе устройства подключены стрелочный индикатор для визуального контроля уровня и излучения или головные телефоны для работы в режиме монитора.

Стрелочная измерительная головка должна быть с током полного отклонения 1 мА и сопротивлением рамки не менее 1 кОм. Микросхему желательно использовать с полевыми транзисторами на входе, такую как К140УД8.

Диод VD1 должен быть обязательно германиевый, типа Д9, ГД 507. Антенна WA — медный провод длиной 30 см.

Индикатор поля, построенный на двух микросхемах, с рабочим диапазоном частот 20—1300 МГц

Индикатор поля на двух микросхемах, схема которого представлена на **рис. 7.2**, немного сложнее по конструкции, но значительно удобнее в работе. Прибор удобно использовать для контроля за рабо-

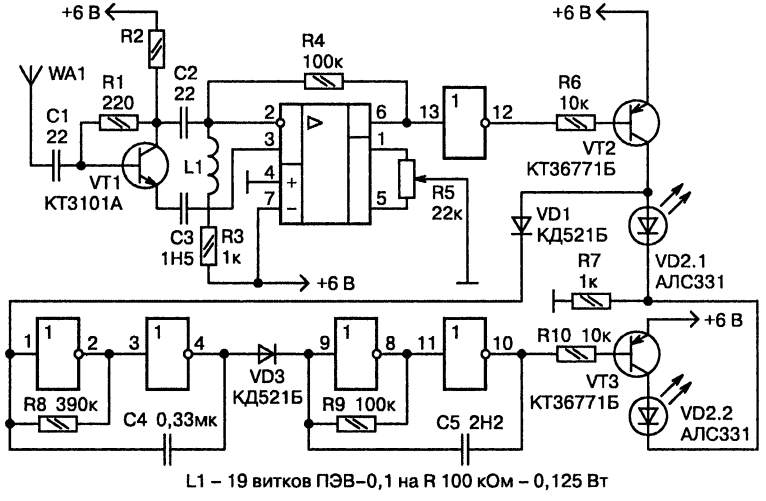


Рис. 7.2. *Схема простого индикатора поля*

той и настройки маломощных передающих устройств, работающих в широком диапазоне частот. Схему также представил на сайте http://cxem.net tolik777 (aka Viper).

Рабочая частота составляет 20—1300 МГц, чувствительность — 1 мВ, пределы локализации лежат в пределах 0,05—7 м. Напряжение питания 4,5—9 В, а ток потребления не превышает 8 мА. Прибор имеет телескопическую антенну.

Это устройство **предназначено** для локального поиска радиозакладок. Его **отличительными особенностями** являются:

- простота повторения;
- надежность;
- малые габариты.

Это интересно знать.

И этот прибор имеет недостаток — немного реагирует на посторонние излучения радиоэфира от телерадиопередающих станций, радиотелефонов. Но этот недостаток с лихвой компенсируется простотой и дешевизной индикатора.

Входной сигнал, наведенный телескопической антенной, поступает на входной усилитель ВЧ, построенный на транзисторе VT1, и далее, через фильтр C1, L1, C3 на детектор-компаратор DA1.

Порог включения компаратора устанавливается резистором R5. Сигнал компаратора с выхода 6 через инвертор DD1.3 и ключ VT2 управляет генератором прямоугольных импульсов на элементах DD1.4, DD1.5 с частотой 1 Гц, который, в свою очередь, включает генератор звуковой частоты на DD1.1, DD1.2.

Светодиод VD1 — двухцветный:

- VD1.1 сигнализирует о включении питания зеленым светом;
- VD2.2 сигнализирует об обнаружении источника радиоизлучений красным светом.

Настройка прибора заключается в выборе ОУ DA1 с возможно большим коэффициентом усиления.

Это интересно знать.

Расстояние, на котором индикатор должен устойчиво реагировать, имея антенну длиной 30 см, на радиопередатчик мощностью 1 мВт, должно быть не менее 50 см.

Транзистор КТ3101 можно заменить на КТ371, КТ368 с коэффициентом усиления не менее 150. Операционный усилитель — К140УД608, К140УД708.

Светодиод АЛС331 можно заменить обычными, типа АЛ307, включив их вместо VD1.1 и VD1.2. Катушка индуктивности имеет 19 витков, намотанных в ряд на любом резисторе МЛТ 0,125, проводом ПЭЛ-0,1.

Простой индикатор поля на ИМС 548УН1А с широким диапазоном поиска от 20 кГц до 500 МГц

Этот простой детектор «радиозакладок» (радиомикрофонов, радиотранслятров и т. п.) позволяет найти «жучки», работающие на частотах от нескольких десятков килогерц до 500 мегагерц. Схему (**рис. 7.3**) разработал Евгений Лесовой (http://cxem.net).

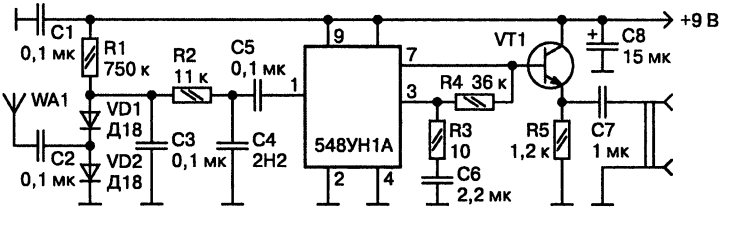


Рис. 7.3. Схема простого индикатора поля

Антенна — кусок провода, длиной около 40 см. Выход на наушники от плеера (низкоомные). Питание от батареи «Крона».

Простой малогабаритный индикатор поля с индикацией на двух светодиодах

Простой малогабаритный **детектор жучка с индикацией на двух светодиодах** отличается малыми габаритами, малым количеством используемых деталей и, вместе с тем, достаточно высокой чувствительностью.

Основу данного устройства составляет микросхема DA1 типа КР1112ПП2. Эта микросхема включает в себя устройство определения баланса электрического моста с индикацией. Микросхема имеет встроенный источник опорного напряжения. Принципиальная схема детектора представлена на **рис. 7.4.**

Сигнал, наводимый в антенне, усиливается широкополосным апериодическим усилителем высокой частоты на транзисторе VT1 типа КТ3101. Усиленное переменное напряжение высокой частоты через конденсатор C3 поступает в диодно-резистивный мост на диодах VD1—VD4 типа ГД507 и резисторах R3—R5.

От источника опорного напряжения (вывод 3 микросхемы DA1) через резисторы R3—R5 и диоды VD1—VD4 протекает небольшой (примерно несколько микроампер) прямой ток, который улучшает условия детектирования и увеличивает чувствительность детектора.

В выпрямлении измеряемого переменного напряжения участвуют только диоды VD1 и VD2, а два других — VD3, VD4 — образуют сосед-

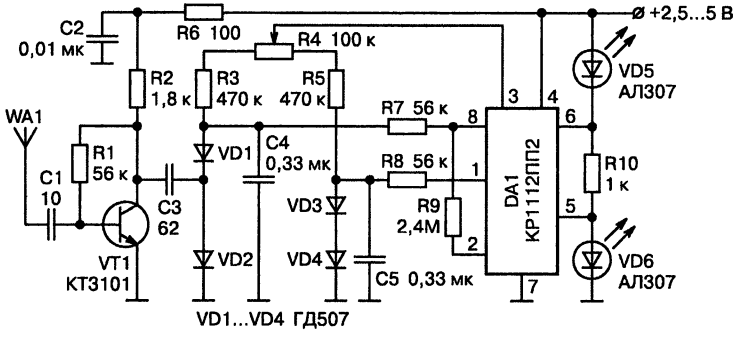


Рис. 7.4. Принципиальная схема детектора жучков с индикацией на двух светодиодах

нее плечо моста, на котором создается начальное напряжение, балансирующее мост, и одновременно служат для его термокомпенсации.

Совет.
Все диоды должны подбираться с возможно более близкими вольт-амперными характеристиками.

Конденсатор С4 от фильтровывает переменную составляющую выпрямленного напряжения. Резистор R4 служит для точной балансировки моста. При хорошей балансировке устройство будет реагировать только на напряжение, являющееся результатом выпрямления измеряемого сигнала.

Выпрямленное напряжение и напряжение, балансирующее мост, через резисторы R7 и R8 поступают на входы усилителя постоянного тока, расположенного в микросхеме DA1.

В зависимости от состояния баланса моста сигнал индикации поступает на один из светодиодов VD5 или VD6 (типа АЛ307):

- при балансе моста (отсутствие сигнала) включен светодиод VD5;
- при наличии сигнала (нарушение баланса моста) включен светодиод VD6.

В качестве диодов VD1—VD4 можно использовать любые высокочастотные диоды. В качестве источника питания используется источник постоянного тока напряжением 2,5—5 В.

Простой детектор радиоволн со звуковой индикацией и рабочим диапазоном поиска до 500 МГц

Простейшее устройство для поиска «жучков» представляет собой детектор радиоволн со звуковой индикацией. С его помощью можно отыскать в помещении работающий микропередатчик.

Это интересно знать.
Этот детектор радиоволн чувствителен к частотам вплоть до 500 МГц.

Настраивать детектор при поиске работающих передатчиков можно путем изменения длины телескопической приемной антенны. Телескопическая приемная антенна воспринимает высокочастотные

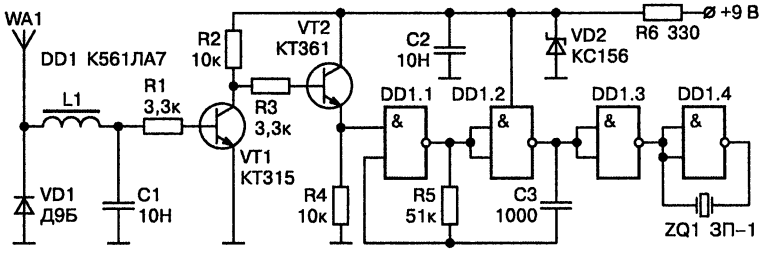


Рис. 7.5. Схема детектора радиоволн на ИМС К561ЛА7

электромагнитные колебания в диапазоне до 500 МГц, которые затем детектируются диодом VD1 типа Д9Б.

Принципиальная схема устройства приведена на рис. 7.5.

Схема работает следующим образом. Высокочастотная составляющая сигнала отфильтровывается дросселем L1 и конденсатором C1. Низкочастотный сигнал поступает через резистор R1 на базу транзистора VT1 типа КТ315, что приводит к открыванию последнего и, как следствие, к открыванию транзистора VT2 типа КТ361.

При этом на резисторе R4 появляется положительное напряжение, близкое к напряжению питания, которое воспринимается логическим элементом DD1.1 микросхемы DD1 типа К561ЛА7 как уровень логической единицы.

При этом включается генератор импульсов на элементах DD1.1, DD1.2, R5 и C3, с выхода которого импульсы с частотой 2 кГц поступают на вход буферного каскада на элементах DD1.3, DD1.4.

Нагрузкой этого каскада служит звуковой пьезокерамический преобразователь ZQ1 типа ЗП-1, который преобразует электрические колебания частотой 2 кГц в акустические. С целью увеличения громкости звучания преобразователь ZQ1 включен между входом и выходом элемента DD1.4 микросхемы DD1.

Питается детектор от источника тока напряжением 9 В через параметрический стабилизатор на элементах VD2, R6.

В детекторе используются резисторы типа МЛТ-0,125. Диод VD1 можно заменить на ГД507 или любой германиевый высокочастотный. Транзисторы VT1 и VT2 могут быть заменены на КТ3102 и КТ3107, соответственно. Стабилитрон VD2 может быть любым с напряжением стабилизации 4,7—7,0 В. Пьезокерамический преобразователь ZQ1 можно заменить на ЗП-22. Индуктивность L1 — 1 мГн. Подробности на http://cxem.net.

Пассивный индикатор электромагнитного высокочастотного поля с частотой поиска до 100 МГц

Далее рассмотрим **пассивный индикатор электромагнитного высокочастотного поля**, принципиальная схема которого представлена на **рис. 7.6, *а***. При минимуме деталей и отсутствии активных компонентов он показывает действительно уровень поля, а не возможные неполадки своей электронной схемы.

Главным элементом для изготовления индикатора высокочастотного излучения является сверхвысокочастотный детекторный диод. В качестве такого диода могут быть применены старые (скорее всего точечные) СВЧ диоды типа Д405, Д602 или подобные, СВЧ детекторные диоды Шотки КА202— КА207, импортные детекторные СВЧ диоды. В крайнем случае, для пробы можно взять германиевый диод вроде Д311, но его рабочая частота не превысит 100 МГц.

Главным отличием детекторного диода является то, что прямая ветвь его вольтамперной характеристики начинает подниматься почти сразу от 0 В.

Будьте осторожны.
Ни в коем случае не следует измерять СВЧ диоды тестером.

Любознательные, не имеющие характериографа, могут снять характеристику диода вручную с использованием вольтметра и миллиамперметра, подавая на диод прямое напряжение с шагом 0,05 В и ограничивая постоянный ток через него величиной не более 0,5 мА.

Когда диод найден, можно приступать к изготовлению индикатора. Собственно, самим индикатором выступает стрелочный микроамперметр PA1 с пределом измерения тока 30—50 мкА. Кремниевые диоды VD1, VD2 защищают детектор и индикатор от перегрузки.

Антенной WA1 могут служить проволочные «усы» из медного провода диаметром 1—2 мм длиной по 200—300 мм или две телескопические антенны. Для большей чувствительности индикатора длина антенны должна быть близка к полуволне измеряемого излучения.

С помощью пассивного индикатора поля удобно исследовать поведение передатчиков, оценивать диаграммы направленности антенн, но для обследования помещений пассивный индикатор неудобен. Он имеет невысокую чувствительность, размахивая таким индикатором, поэтому затруднительно увидеть изменение положения стрелки при-

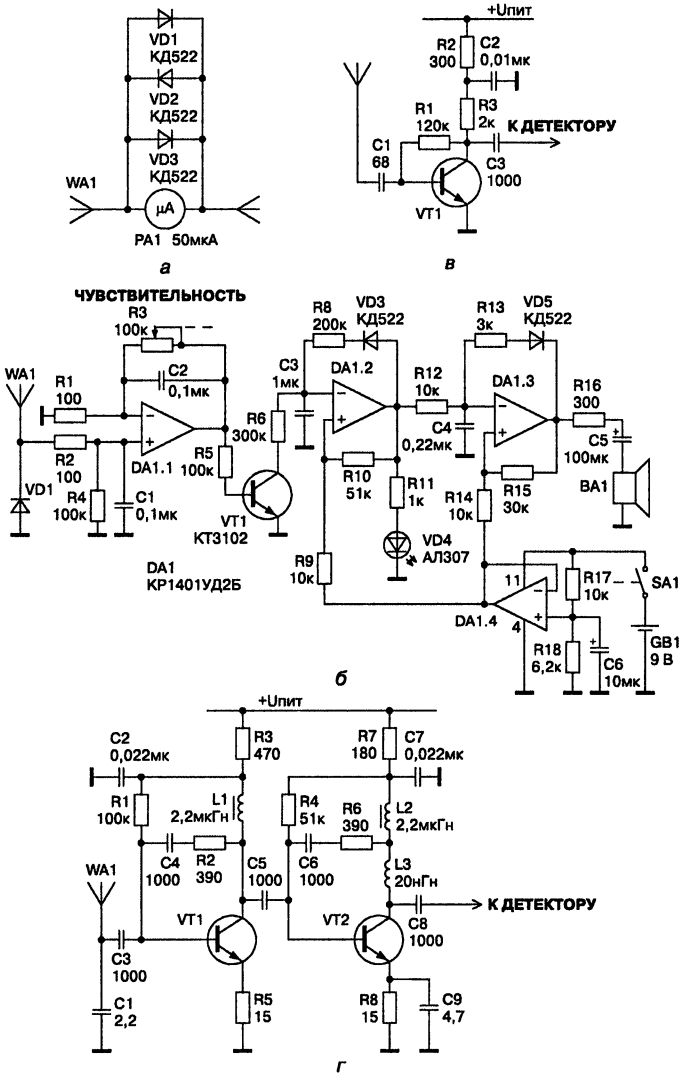


Рис. 7.6. *Индикаторы поля:*

а — принципиальная схема пассивного индикатора поля;

б — принципиальная схема индикатор поля со звуковой индикацией;

в — принципиальная схема простого УВЧ для индикатора поля;

г — принципиальная схема широкополосный стабильный УВЧ для индикатора поля

бора, да и сам высокочувствительный стрелочный микроамперметр очень не любит сотрясений и ударов.

Для удобства применения приходится окружать СВЧ детектор электронной схемой (**рис. 7.6, *б***). Схема осуществляет световую и звуковую индикацию уровня напряженности поля.

Изменение напряженности поля можно оценивать по частоте следования звуковых сигналов длительностью 0,2 мс и частотой около 1 кГц или вспышек светодиода VD4.

Количество сигналов меняется от одного за десятки секунд до непрерывного тона при большом уровне сигнала. Звуковая индикация позволяющая оценивать текущий уровень ВЧ излучения и регулятор чувствительности позволяют быстро и эффективно локализовать источник радиоизлучения.

Первый ОУ DA1.1 является неинвертирующим усилителем постоянного тока, величина усиления которого регулируется резистором R3, совмещенным с выключателем. Следующие два каскада на DA1.2, DA1.3 построены по однотипной схеме управляемого мультивибратора на ОУ. Повторитель на DA1.4 служит формирователем уровня «земли». На DA1.3 собран мультивибратор, управляемый напряжением высокого уровня, его частота около 1000 Гц. Звуковой мультивибратор запускается от генератора управляемого напряжением, выполненного на DA1.2.

Положительные импульсы генератора не зависят от уровня входного сигнала, их длительность около 0,2 с задает цепочка R8, C3. Длительность пауз между импульсами зависит от скорости разряда C3 через транзистор VT1 и резистор R6. А проводимость транзистора VT1 в свою очередь зависит от входного ВЧ напряжения выпрямленного детектором VD1 и увеличенного усилителем постоянного тока на DA1.1. В качестве DA1 используется счетверенный операционный усилитель с диапазоном входных сигналов, включающим нулевое входное напряжение.

Если чувствительность индикатора покажется недостаточной, то перед VD1 можно включить широкополосный высокочастотный усилитель выполненный по схеме приведенной на **рис. 7.6, *в*** или **рис. 7.6, *г***.

Чтобы широкополосный УВЧ не возбуждался и имел равномерную частотную характеристику, он должен быть выполнен с соблюдением требований конструирования высокочастотных устройств.

Совет.
Транзисторы для УВЧ желательно брать с граничной частотой не менее 4 ГГц.

Прибор снабжен телескопической антенной WA1 и питается от девятивольтовой батареи. Переменным резистором R3, совмещенным с выключателем питания SA1, регулируют чувствительность прибора. Его выставляют таким образом, чтобы увеличение уровня напряженности поля вызывало наиболее резкое изменение частоты следования импульсов индикации.

Низкочастотный поисковый индикатор на рабочую частоту до 100 кГц

Низкочастотный поисковый индикатор может быть использован для обнаружения устройств, передающих информацию по проводам. Эти устройства используют приемники сигналов с проводной линии, имеющие диапазон частот, лежащий между звуковыми и радиочастотами. Высшую частоту диапазона такого приемника разумно ограничить величиной 100 кГц. Для этого есть несколько причин:

- **во-первых**, хорошие сканирующие приемники имеют возможность работать в ЧМ, начиная с этой частоты;
- **во-вторых**, при передаче сигнала по проводам ЧМ является наиболее помехозащищенным видом модуляции;
- **в-третьих**, в диапазоне 30—100 кГц самыми дальнобойными являются именно низкие частоты.

Причем передача сигнала на частотах 100 кГц и выше имеет заметное радиоизлучение и может быть обнаружена обычным радиоприемником с диапазоном длинных и средних волн.

Схема низкочастотного индикатора (**рис. 7.7**) представляет собой ЧМ приемник диапазона 25—125 кГц, адаптированный под задачу обнаружения частотно-модулированных сигналов в любой линии. Исследуемая линия подключается через входной трансформатор T1. Он предназначен для гальванической развязки индикатора от линии в целях защиты от поражения электрическим током.

После трансформатора включен полосовой фильтр с частотами среза 30—100 кГц. Фильтр состоит из последовательно включенных фильтра высоких частот на C2, C3, L1 и фильтра низких частот на C4, C5, L2. Фильтры выполнены на пассивных элементах, так как в иссле-

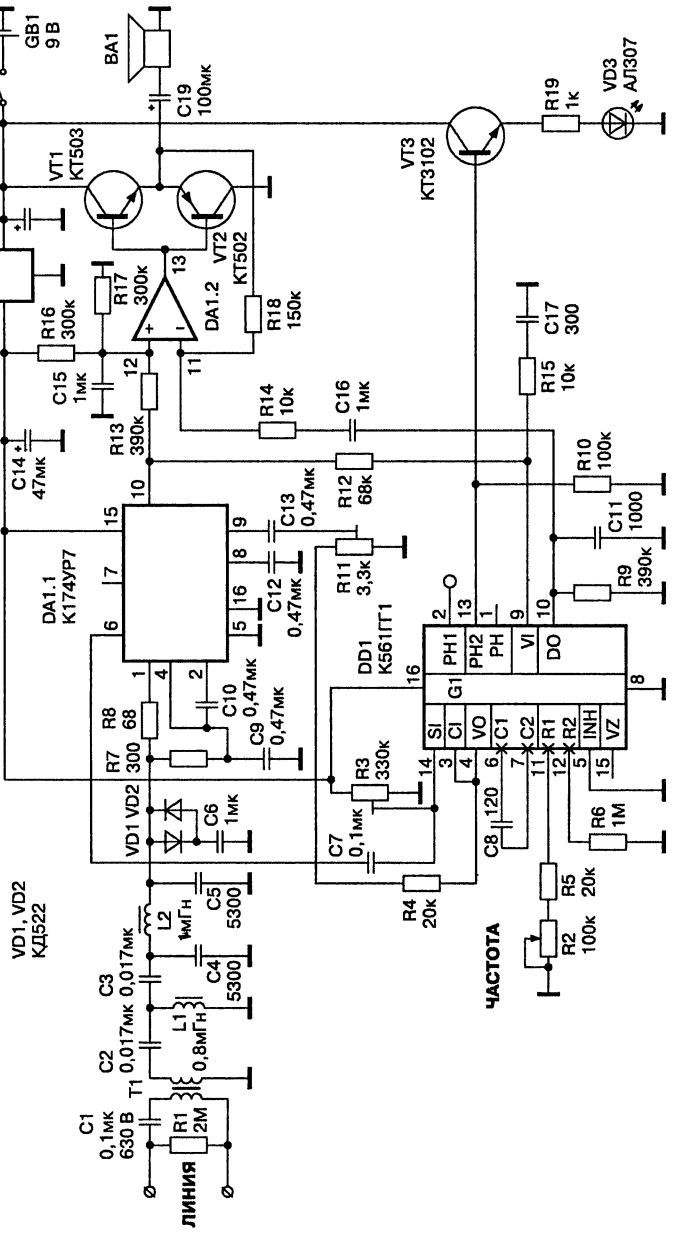


Рис. 7.7. Принципиальная схема обнаружителя низкочастотных сигналов

дуемых линиях может присутствовать высокое переменное напряжение других частот (как, например, в электрической сети).

Далее вся выделенная полоса частот усиливается внутренним усилителем-ограничителем микросхемы DA1. Цепочка VD1, VD2, C6 служит для защиты микросхемы от высоковольтных импульсов. Усиленный и ограниченный сигнал демодулируется частотным детектором с ФАПЧ. Петля фазовой автоподстройки частоты включает генератор управляемый напряжением из состава микросхемы DD1 и фазовый детектор из состава микросхемы DA1.

С выхода 10 DA1 через пропорционально-интегрирующий фильтр на R12, R15, C17 сигнал управления поступает на вход ГУНа. Высокочастотный сигнал ГУНа с выхода 4 DD1 через элементы R4, R11, C13 подается на вход 9 фазового детектора из состава DA1. Входной высокочастотный сигнал подключен к фазовому детектору внутренними цепями DA1.

Это интересно знать.

Фазовые детекторы из состава DD1 не используются при демодуляции звука, один из них только лишь управляет светодиодом индикации VD3 через повторитель на транзисторе VT3. Использование фазового детектора микросхемы DA1 в петле ФАПЧ позволяет получить более качественное детектирование звука.

Демодулированный звуковой сигнал через внутренний истоковый повторитель (выход 10) микросхемы DD1 поступает на усилитель низкой частоты, выполненный на ОУ DA3 и транзисторах VT1, VT2. Отношение резисторов R18, R14 определяет его величину усиления. К выходу УНЧ подключен малогабаритный динамик BA1. Частотная селекция входного сигнала осуществляется ФАПЧ демодулятором, его центральная частота перестраивается переменным резистором R2 от 25 до 125 кГц.

В связи с тем, что усилению подвергается вся рабочая полоса частот, на выходе УНЧ всегда присутствует шум — сильный при отсутствии сигнала, слабый при сильном входном сигнале. Это способствует образованию обратной связи при присутствии передатчика.

Индикаторный светодиод VD3 беспорядочно мигает в отсутствии сигнала. При обнаружении сигнала переходит через потушенное и зажженное состояние при перестройке по частоте резистором R2. Или остается в одном из этих состояний, если петля ФАПЧ удерживает настройку при сильном сигнале.

Индикатор обнаруживает на всех 8 км его дальности действия. Индикатор также позволяет определять присутствие видеосигнала в линии, цифрового сигнала с частотной модуляцией. Исследуемая линия может быть любой двухпроводной линией (телефонная линия, линия компьютерной сети, линия электроснабжения 220 В и т. п.). Ограничение накладывает величина пробивного напряжения, определяемая качеством изоляции между обмотками трансформатора T1 и допустимым напряжением конденсатора C1.

Требования к элементам схемы небольшие: конденсатор C1 обязательно должен быть высоковольтным, C2—C5 составляются из нескольких, имеющих стандартные номиналы.

Трансформатор T1 и катушки L1, L2 намотаны на ферритовых кольцах 20×10×5 проницаемостью 2000НН. T1 имеет по 70 витков в каждой обмотке, L1 — 24 витка, L2 — 27 витков.

Обмотки трансформатора изолированы друг от друга слоем лакотканевой или фторопластовой изоляции. При желании намоточные данные катушек и трансформатора можно пересчитать для сердечников меньшего размера. Индикатор питается от девятивольтовой батареи через интегральный стабилизатор DA2.

Настройка индикатора сводится к установке подстроечным резистором R3 меандра на выводе 2 DD1 и резистором R11 наименее искаженного звукового сигнала на выходе УНЧ. Это лучше сделать при наличии входного сигналов.

Широкополосный детектор радиоволн с рабочей полосой до 1 ГГц

Этот прибор **можно назвать детектором радиоволн** и предназначен для поиска микропередатчиков. Он представляет собой звуковой и световой сигнализатор наличия радиочастотных излучений. Прибор имеет высокую чувствительность в полосе частот до 1 ГГц. Например, «жучок» с излучаемой мощностью 1,5 мВт (выходной каскад на одном маломощном транзисторе) можно обнаружить с расстояния около 10 см.

Конструкция прибора проста и доступна для повторения даже радиолюбителям с небольшим опытом изготовления электронных устройств. В нем использованы доступные компоненты. При этом потребительские свойства этого сигнализатора весьма неплохие. Он

имеет малые размеры и массу, прост в эксплуатации: единственный орган управления — выключатель питания.

Принципиальная схема сигнализатора показана на **рис. 7.8, *а***. Расположение элементов и печатная плата приводятся на **рис. 7.8, *б***.

При приближении антенны WA1 к микропередатчику в ней наводится высокочастотное напряжение, которое через конденсатор C1 поступает на вход УРЧ (транзистор VT1). Емкость конденсатора C1 определяет нижнюю границу принимаемого диапазона частот. Ее подбирают такой, чтобы индикатор не реагировал на бытовые низкочастотные помехи от электродвигателей, тиристорных регуляторов напряжения, ГСП магнитофонов и т. п.

С выхода УРЧ сигнал поступает на диодный детектор VD1. Через фильтр C4 L1 и резистор R6 постоянная составляющая продетектированного сигнала поступает на вход усилителя постоянного тока (транзисторы VT2, VT3).

Резистор R6 несколько снижает чувствительность индикатора, но он необходим для того, чтобы избежать резкого повышения чувствительности прибора на частоте резонанса контура C4 L1 (около 50 кГц).

Усилитель постоянного тока управляет работой мультивибратора на транзисторах VT4 и VT5. К коллекторным цепям транзисторов VT4, VT5 подключен пьезоизлучатель ZQ1, который преобразует электрические колебания, вырабатываемые мультивибратором, в звук. При работе мультивибратора, кроме того, светится и светодиод HL1.

Это интересно знать.
Такое включение излучателя повышает громкость его звучания.

Чем больше мощность сигнала от «жучка», тем больше ток через транзистор VT3 и тем выше частота звукового сигнала и его громкость, а также интенсивность свечения светодиода HL1. Перемещая сигнализатор, ищут его положение, при котором максимальны громкость сигнала и яркость светодиода.

Затем уже в «ближней зоне» проводят визуальный поиск местонахождения подслушивающего устройства.

На диод VD1 через резистор R4 поступает напряжение смещения со стабилизатора напряжения R5, VD6, которое приоткрывает диод VD1 и транзистор VT2. Это повышает чувствительность детектора к малым уровням ВЧ сигналов.

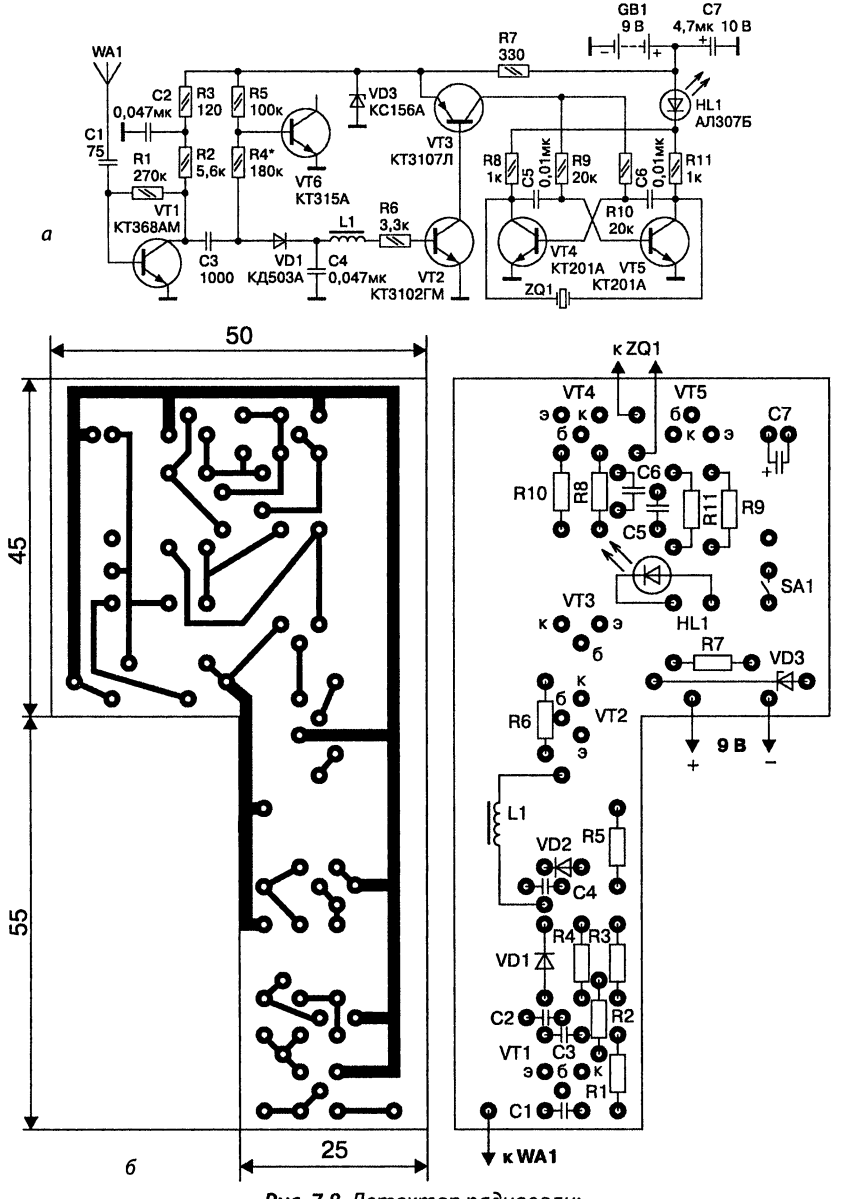


Рис. 7.8. *Детектор радиоволн:*
а — принципиальная схема; б — печатная плата и расположение элементов

Совет.

Резистор R4 нужно подбирать так, чтобы светозвуковой сигнализатор находился на грани срабатывания сигнализатора.

Как следствие, даже очень небольшая добавка напряжения, возникающая при детектировании исследуемого сигнала, открывает транзисторы VT2, VT3, запуская мультивибратор.

Это интересно знать.

***Недостаток** такого решения — заметная термочувствительность сигнализатора. Ее можно устранить, подобрав R4 так, чтобы сигнализатор не срабатывал самопроизвольно в выбранном диапазоне температуры.*

Облегчит эту процедуру применение в качестве VT2 транзистора с очень малым обратным током.

Диод VD1 можно заменить на КД503Б, КД509А, КД512А, КД407А или КД409А. Стабилитрон VD3 — любой с напряжением стабилизации 5—7 В. Транзистор VT1 — КТ368 с любым буквенным индексом в любом корпусе либо другой высокочастотный, например, КТ3101А-2, КТ3120А, КТ3124.

Транзистор VT2 — КТ3102 с индексами Г, Е. Заменять его другими не стоит, так как он имеет очень малый начальный ток коллектор-эмиттер — менее 0,05 мкА. Транзистор VT3 можно заменить на КТ3107 с индексами К, Д.

Вместо транзисторов VT4 и VT5 допускается использовать любые кремниевые маломощные транзисторы соответствующей структуры с подходящей цоколевкой. Лишь бы обратный ток коллектора был достаточно мал, чтобы мультивибратор не самовозбуждался. По этой причине нельзя применять германиевые транзисторы. Чем больше коэффициент передачи тока каждого транзистора, тем выше чувствительность всего устройства.

В качестве пьезоэлемента использован пьезоизлучатель ZQ1, например, от электронных часов «Монтана», но здесь подойдут и любые другие. Дроссель L1 должен иметь индуктивность 1—2 мГн. Он содержит 180 витков провода ПЭЛШО-0,12 на кольце от импульсного трансформатора ТИ-18. Выключатель SA1 — ПД9-2. Антенна WA1 — телескопическая от импортной магнитолы общей длиной 32 см.

Совет.
Слишком длинную антенну использовать не следует.

Наладку сигнализатора начинают с установки напряжения смещения на диоде VD1. Для этого конденсатор C3 нужно временно отключить. Вместо резистора R4 временно устанавливают переменный сопротивлением 560 кОм. Вращая его движок, добиваются исчезновения звука.

Если теперь поднести устройство к лампе накаливания или вынести на солнечный свет, то сигнализатор начнет слабо пищать, набирая громкость с нагревом. Затем измеряют сопротивление переменного резистора и устанавливают резистор R4 с сопротивлением, в полтора раза большим. Это обеспечит работоспособность сигнализатора радиоизлучения в приемлемом диапазоне температуры. Усиление УРЧ регулируют подбором резистора R2.

Индикатор излучения с полосой поиска от 5 до 300 МГц

Индикаторы излучения рассматриваются на http://cadlab.ru/content/view/455/31/1/3/. В индикаторе используется диод с барьером Шоттки КД514. При его монтаже с целью исключения выхода его из строя нужно применять защиту от статического электричества.

В простейшем случае антистатический браслет может быть изготовлен из металлического браслета для часов, к которому с помощью зажима «крокодил» прикрепляется резистор номиналом 100 кОм...1 МОм. Второй конец резистора соединяется с контуром заземления или с водопроводной трубой холодной воды. Корпус паяльника также необходимо заземлить.

Настройка ВЧ-индикатора. При подготовке детектора к работе установите движок подстроечного резистора R9 в крайнее левое положение (максимальная чувствительность) и включите питание. Вращая ручку переменного резистора R10, нужно добиться генерации самого низкочастотного тона в отсутствие электромагнитного излучения.

Теперь можно обследовать помещение. При приближении к источнику электромагнитного поля частота тона будет повышаться. При перегрузке детектора резистором R9 уменьшите его чувствительность.

Громкость сигнала можно изменить увеличением или уменьшением номинала резистора R26.

В проверяемом помещении необходимо выключить все известные источники электромагнитного излучения: люминесцентные лампы, компьютеры, радиоприемники и все виды телефонов. В противном случае они затруднят поиск «жучков».

С помощью индикатора можно обнаружить передающие устройства, работающие в диапазоне 5—300 МГц. Например, передатчик мощностью 10 мВт можно обнаружить на расстоянии 20—25 см.

Технические характеристики:

- напряжение питания, В.....9;
- ток потребления, мА .....18—30;
- диапазон рабочих частот, МГц .....5—300.

Электрическая схема индикатора приведена на **рис. 7.9.**

Индикатор ВЧ-излучения функционально состоит из пяти каскадов. Первый каскад — широкополосный усилитель высокой частоты собранный по схеме с коллекторной стабилизацией рабочей точки на транзисторе VT1. Второй каскад — детектор на диоде Шоттки VD1 Третий — компаратор на операционном усилителе ОУ1 из состава ИС DA1.

На ОУ2—ОУ4 и VT3 собран четвертый каскад — перестраиваемые генератор низкой частоты, управляемый напряжением (ГУН).

ГУН выполнен по классической схеме, содержащей каскады интегратора, компаратора и разрядного транзистора. Интегратор собран на ОУ3, компаратор — на ОУ4. Скорость заряда конденсатора С10 зависит от величины напряжения на входе ГУН (точка соединения резисторов R16 и R17).

Как только напряжение на выходе интегратора достигает порога срабатывания компаратора ОУ4, открывается разрядный транзистор VT3. После разряда конденсатора С10 цикл начинается заново.

На ОУ2 собран буферный каскад для предотвращения влияния входной цепи ключевого усилителя звуковой частоты, собранного на транзисторе VT2 (пятый каскад), на стабильность работы ГУН.

Будьте осторожны.

В индикаторе используется диод с барьером Шоттки КД514. При его монтаже с целью исключения выхода его из строя нужно применять защиту от статического электричества.

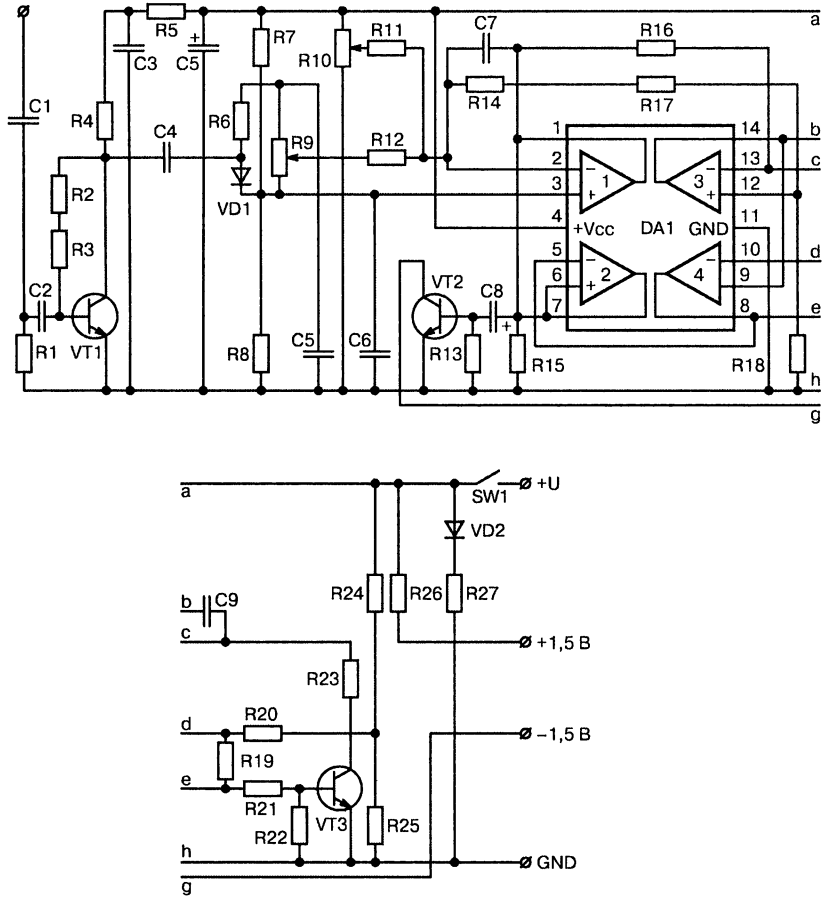


Рис. 7.9. *Электрическая схема индикатора ВЧ излучения*

В простейшем случае антистатический браслет может быть изготовлен из металлического браслета для часов, к которому с помощью зажима «крокодил» прикрепляется резистор номиналом 100 кОм ... 1 МОм. Второй конец резистора соединяется с контуром заземления или с водопроводной трубой холодной воды. Корпус паяльника также необходимо заземлить.

Совет.

В проверяемом помещении необходимо выключить все известные источники электромагнитного излучения: люминесцентные лампы, компьютеры, радиоприемники и все виды телефонов. В противном случае они затруднят поиск «жучков».

Настройка ВЧ-индикатора. При подготовке детектора к работе установите движок подстроечного резистора R9 в крайнее левое положение (максимальная чувствительность) и включите питание. Вращая ручку переменного резистора R10, нужно добиться генерации самого низкочастотного тона в отсутствие электромагнитного излучения.

Теперь можно обследовать помещение. При приближении к источнику электромагнитного поля частота тона будет повышаться.

Совет.

При перегрузке детектора резистором R9 уменьшите его чувствительность.

Громкость сигнала можно изменить увеличением или уменьшением номинала резистора R26.

Индикатор излучения сотового телефона в диапазоне СВЧ

Индикатор излучения сотового телефона в диапазоне СВЧ рассмотрен на http://radiomaster.com.ua/index.php?newsid=164. В отличие от описанного в журнале «Радио» аналогичного устройства (Виноградов Ю. Детектор излучения сотового телефона. — Радио, 2004, № 2, с. 43), предлагаемый индикатор имеет значительно больший радиус действия, достигающий 10 м. Схема устройства показана на **рис. 7.10**. Прием сигнала ведется на широкополосную полуволновую антенну, состоящую из двух вибраторов W1 и W2.

Прибор выполнен по схеме приемника прямого усиления и содержит усилитель радиочастоты (УРЧ), детектор и звуковой индикатор. Сигнал, наведенный в приемной антенне, усиливается УВЧ и поступает на детектор. Продетектированный сигнал открывает электрон-

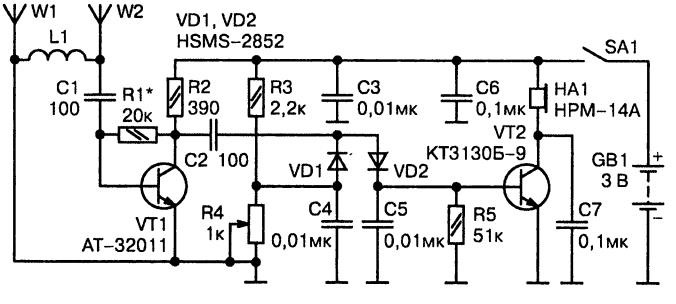


Рис. 7.10. Индикатор излучения сотового телефона в диапазоне СВЧ

ный ключ, собранный на транзисторе VT2, а он, в свою очередь, включает звуковой сигнализатор HA1 — зазвучит сигнал.

С помощью индикатора удается определять и режимы работы сотового телефона. Когда сотовый телефон входит в сеть, индикатор подает короткие звуковые сигналы, а при вызове абонента и при разговоре с ним звуковой сигнал звучит непрерывно.

Радиочастотный искатель подслушивающих устройств в диапазоне 30—500 МГц

Радиочастотный искатель подслушивающих устройств рассмотрен на http://www.irls.narod.ru/sig/isk/abag04.htm. Сегодня все чаще можно столкнуться с применением в различных целях радиомикрофонов и телефонных радиопрослушивающих устройств. Иногда необходима уверенность в том, что разговор в квартире или офисе не прослушивается. Обычно радиоподслушивающие устройства («жучки») излучают на одной частоте в диапазоне 30—500 МГц небольшую мощность (до 5 мВт).

Иногда такие устройства работают в ждущем режиме: включаются на передачу при наличии шума в помещении (что обеспечивает экономичность расходования энергии элементов питания) или же при снятии телефонной трубки.

Простейшее устройство, которое способно помочь в обнаружении подслушивающих устройств, приведено на **рис. 7.11**.

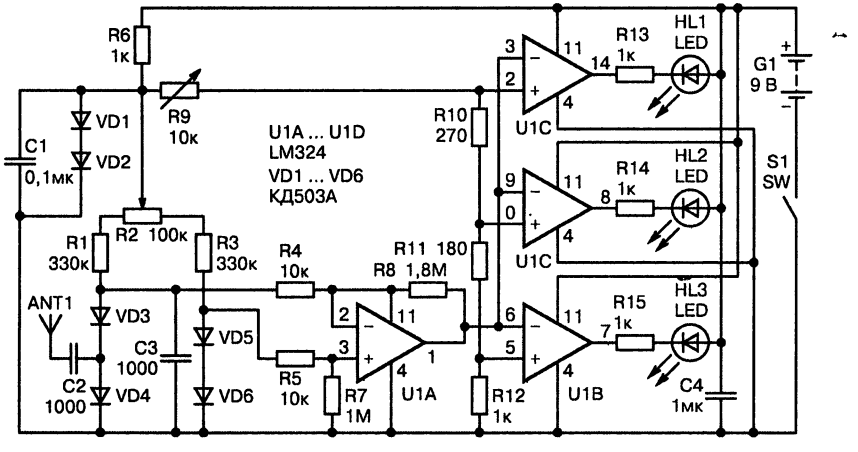


Рис. 7.11. Радиочастотный искатель подслушивающих устройств

Схема является широкополосным мостовым детектором ВЧ напряжения. Он перекрывает диапазон частот 1—200 МГц (при использовании в качестве D01—D06 диодов СВЧ диапазона рабочая полоса может быть расширена) и позволяет обнаруживать «жучки» на расстоянии примерно 0,5—1 м (это зависит от мощности передатчика).

Это интересно знать.
Известно, что измерение ВЧ напряжений с уровнем меньше 0,5 В затруднено тем, что уже при 0,2—0,3 В все полупроводниковые диоды при детектировании становятся неэффективны из-за особенности их вольтамперной характеристики.

В данной схеме применен известный способ измерения малых переменных напряжений с использованием **сбалансированного диодно-резистивного моста**. Небольшой ток, протекающий через диоды D3, D4, улучшает условия детектирования (повышает чувствительность) и позволяет отодвинуть нижнюю границу уровня измеряемых напряжений до 20 мВ при равномерной амплитудно-частотной характеристике.

Диоды D5, D6 образуют второе плечо моста и обеспечивают термостабилизацию схемы. На элементах микросхемы U1.2—U1.4 собраны трехуровневые компараторы, к выходам которых подключены светодиодные индикаторы HL1—HL3.

Диоды D1, D2 применены как стабилизаторы напряжения 1,4 В, что необходимо для устойчивой работы схемы в широком диапазоне изменения питающих напряжений.

Это интересно знать.
Применение устройства *требует определенных навыков, так как схема довольно чувствительна и способна улавливать вблизи любые радиоизлучения, например, работу гетеродина приемника или телевизора, а также вторичное переизлучение токопроводящими поверхностями.*

Для облегчения поиска «жучка» используют сменные антенные штыри с разной длиной, которые позволяют снизить чувствительность схемы. Например, возможно применение сменных штырей длиной 400—700—1200 (мм).

При использовании устройства, после его включения, необходимо резистором R2 добиться свечения индикатора HL3. Этим устанавли-

вается **уровень начальной чувствительности** относительно фона. При поднесении антенны к источнику радиоизлучения должны начинать светиться светодиоды HL2 и HL1 по мере увеличения амплитуды принятого сигнала.

Регулировку схемы подстроечным резистором R9 выполняют один раз (при первоначальной настройке устройства от него зависит уровень порогов чувствительности компараторов). Схема сохраняет работоспособность при изменении питания от 6 до 10 В.

Детектор жучков с логарифмической шкалой на 12 светодиодах и звуковой индикацией

Детектор жучков с логарифмической шкалой на 12 светодиодах и звуковой индикацией рассмотрен на http://www.radioland.net.ua/sxemaid-62.html. В состав детектора поля входят ФВЧ, усилитель ВЧ, диодный детектор, усилитель постоянного тока с логарифмической зависимостью коэффициента усиления, звуковой генератор с изменяющейся частотой и светодиодная шкала из 12 светодиодов.

Детектор способен регистрировать работающие радиомикрофоны в диапазоне частот 20—600 МГц. Принципиальная схема прибора приведена на **рис. 7.12.**

Сигнал, наводимый в антенне, фильтруется ФВЧ на элементах C2, L1, C3, L2 и поступает на широкополосный апериодический усилитель. Последний выполнен на высокочастотном транзисторе VT1 типа КТ3101.

Нагрузкой усилителя служит эмиттерный повторитель на транзисторе VT2 типа КТ3101. Сигнал, снимаемый с регулятора чувствительности — резистора R4, поступает через конденсатор C6 на диодный детектор, собранный на диоде VD1 типа Д9Б.

Высокочастотные составляющие фильтруются RC-фильтрами R5, C7 и R6, C8. Низкочастотный сигнал поступает на усилитель на микросхеме DA1 типа КР140УД1208. Коэффициент усиления этого усилителя определяется значением резистора R9. При малом уровне входного сигнала усилитель на DA1 имеет большое усиление. По мере увеличения сигнала происходит открывание диода VD2 типа КД522, сопротивление которого изменяется по логарифмическому закону. Это приводит к изменению сопротивления обратной связи также по логарифмическому закону. С выхода усилителя на микросхеме DA1 сигнал поступает на светодиодный индикатор и звуковой генератор.

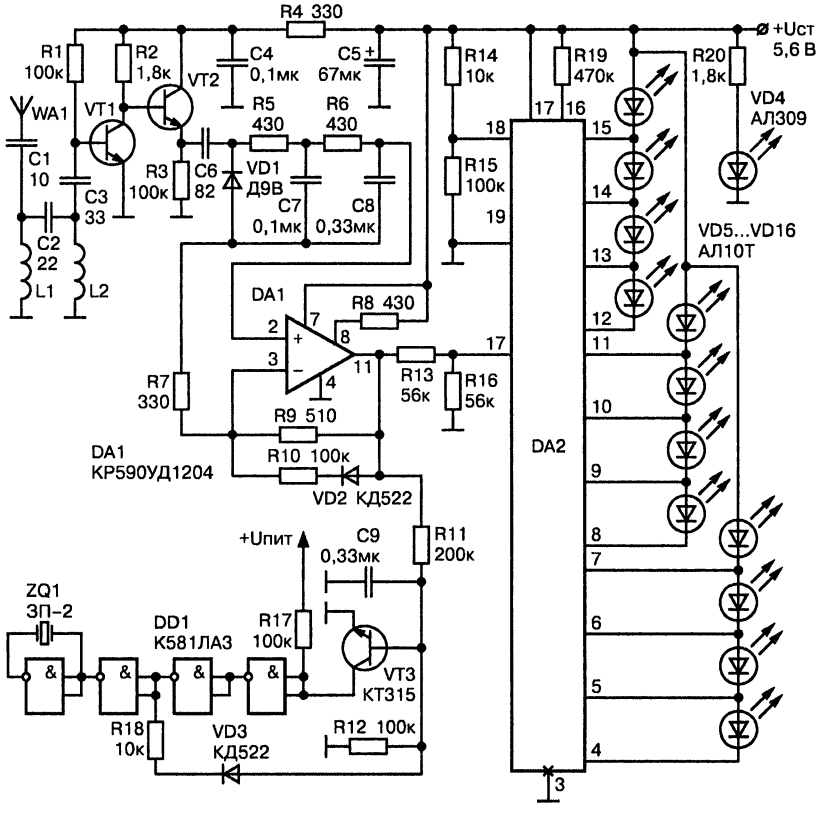


Рис. 7.12. *Детектор жучков с логарифмической шкалой на 12 светодиодах и звуковой индикацией*

Звуковой генератор выполнен на транзисторе VT3 типа КТ315 и микросхеме DD1 типа К561ЛА7. Конденсатор C9 заряжается через резистор R11 до напряжения открывания транзистора VT3. Это приводит к смене уровня логической единицы на уровень логического нуля на коллекторе транзистора VT3. При этом катод диода VD3 типа КД522 оказывается подключенным через резистор R18 к минусу источника питания.

Конденсатор C9 быстро разряжается через цепь VD3, R18,что ведет за собой закрывание транзистора VT3. Конденсатор C9 снова начинает заряжаться и весь процесс повторяется. Прямоугольные импульсы преобразуются пьезокерамическим преобразователем ZQ1 типа ЗП-22 в звуковые.

При увеличении напряжения на выходе усилителя DA1 уменьшается время заряда конденсатора C9 до напряжения открывания тран-

зистора VT3, а это, в свою очередь, приводит к увеличению частоты следования импульсов генератора. Таким образом, при увеличении уровня входного сигнала происходит повышение тональности звукового сигнала.

Основой светодиодного индикатора является микросхема DA2 типа КМ1003ПП2. Микросхема КМ1003ПП2 является специализированной и выполняет функцию управления светодиодной шкалой, обеспечивая высвечивание столбика на шкале из 12 светодиодов, которые загораются поочередно при изменении входного напряжения от минимального до максимального значения. Яркость свечения светодиодов поддерживается постоянной.

Входной сигнал, через делитель напряжения на резисторах R13, R16, поступает на вход микросхемы DA2 (вывод 17). На выводы 16 и 3 микросхемы DA2 подаются уровни опорного напряжения, определяющие, соответственно, минимальное (светодиоды не горят) и максимальное (горят все светодиоды) значения входного сигнала.

Питается устройство от источника питания напряжением 5,6 В. Светодиод VD4 типа АЛ307 служит для индикации включения прибора.

Все используемые детали малогабаритные. Детали ФВЧ описаны выше. Микросхема DA1 может быть заменена на КР1407УД2 или любой другой операционный усилитель со своими цепями коррекции. Вместо микросхемы DD1 можно применить К561ЛЕ5. При замене диода VD1 на ГД507 диапазон прибора может быть увеличен до 900 МГц.

Детектор жучков с линейной шкалой из восьми светодиодов, регулировкой чувствительности и звуковой индикацией

Детектор жучков с линейной шкалой из восьми светодиодов, регулировкой чувствительности и звуковой индикацией представлена на http://cxem.net/indicator/indicator5.php.

Отличительной особенностью данного детектора поля является: фильтр высокой частоты на входе, усилитель постоянного тока на двух операционных усилителях, звуковой генератор, линейная светодиодная шкала и индикатор разряда батареи. Все это делает данное устройство, несомненно, более простым и удобным в эксплуатации. Принципиальная схема детектора поля приведена на **рис. 7.13**.

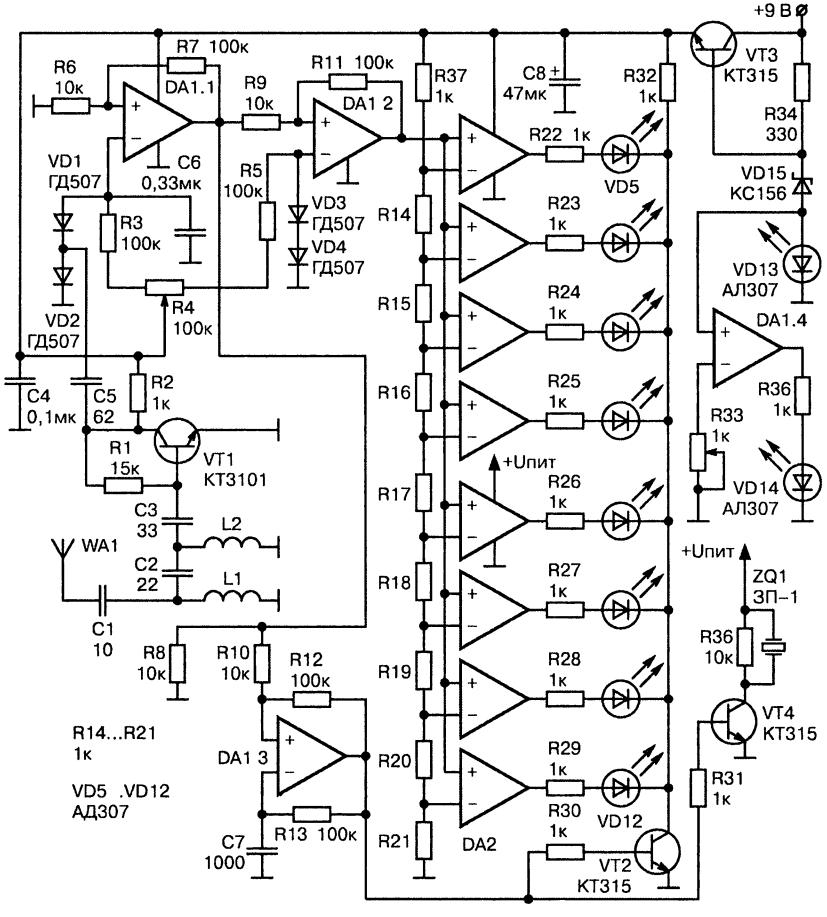


Рис. 7.13. *Детектор жучков с линейной шкалой из восьми светодиодов, регулировкой чувствительности и звуковой индикацией*

Сигнал, принимаемый антенной, поступает на фильтр высокой частоты на элементах C2, L1, C3, L2, необходимый для подавления сигналов частотой менее 20 МГц.

Это интересно знать.

Это необходимо для уменьшения уровня низкочастотных сигналов, обычно составляющих фоновое радиоизлучение.

С ФВЧ сигналы частотой более 20 МГц поступают на вход апериодического широкополосного усилителя высокой частоты, собранного на транзисторе VT1 типа КТ3101. С нагрузки усилителя (резистора R2)

напряжение высокой частоты через конденсатор С5 по ступает на диоды VD1, VD2 типа ГД507, входящие в состав резистивно-диодного моста.

Для балансировки моста используется резистор R4. Продетектированное низкочастотное напряжение, сглаженное конденсатором С6, поступает на усилитель постоянного тока, выполненный на двух операционных усилителях DA1.1 и DA1.2, входящих в состав микросхемы К1401УД1.

С выхода элемента DA1.1 постоянное напряжение поступает на генератор звуковой частоты, выполненный на операционном усилителе DA1.3. Частота генератора зависит от уровня постоянного напряжения на неинвертирующем входе элемента DA1.3, которое, в свою очередь, зависит от уровня входного сигнала.

Это интересно знать.

Таким образом, чем больше уровень входного сигнала, тем выше частота генератора звуковой частоты.

С выхода генератора звуковой сигнал поступает на базу транзистора VT4 типа КТ315, в коллекторную цепь которого включен пьезокерамический преобразователь ZQ1 типа ЗП-1.

Микросхемы DA2 и DA3 типа К1401УД1 составляют основу линейной шкалы. Операционные усилители, входящие в состав этих микросхем, включены по схеме компараторов напряжения. На неинвертирующие входы этих компараторов поступает опорное напряжение с линейки резисторов R14—R21.

Другие входы компараторов соединены вместе, на них поступает постоянное напряжение с выхода усилителя постоянного тока DA1.2. При изменении этого напряжения от нуля до максимального значения происходит переключение компараторов, на выходе которых включены светодиоды VD5—VD14, образующие линейную светоизлучающую шкалу. Чем выше уровень сигнала на входе, тем больше светодиодов включено.

Для уменьшения потребляемого светодиодной шкалой тока используется **принцип динамической индикации**. Для этого на базу транзистора VT2 типа КТ315 поступают импульсы с генератора звуковой частоты DA1.3, вызывая поочередное закрывание и открывание транзистора VT2.

При закрывании транзистора VT2 положительное напряжение источника питания через резистор R32 поступает на катоды свето-

диодов VD5—VD14, что приводит к запиранию последних. Ток через светодиоды не течет и они гаснут.

При открывании транзистора VT2 катоды светодиодов замыкаются на минус источника питания, и те светодиоды, на аноде которых присутствует положительное напряжение, загораются. Благодаря инерционным свойствам человеческого глаза мигание светодиодов становится незаметным.

Индикатор разряда батареи выполнен на элементе DA1.4 и светодиодах VD13, VD14. При снижении напряжения источника питания уменьшается ток, протекающий через стабилитрон VD15 и светодиод VD13 и, соответственно, напряжение на аноде VD13. Это вызывает включение светодиода VD14. Уровень срабатывания устанавливается подстроечным резистором R33 при настройке. Все устройство питается от стабилизатора, собранного на элементах VT3, VD15, VD13, R34, C8.

Детали. В устройстве использованы резисторы типа МЛТ-0,125. Светодиоды VD5—VD14 могут быть любыми. Диоды VD1—VD4 — любые высокочастотные германиевые. Катушки L1 и L2 бескаркасные, диаметром 8 мм, намотанные проводом ПЭВ 0,6 мм. Катушка L1 — 8 витков, катушка L2 — 6 витков. Резистор R4 — любой переменный резистор с линейной характеристикой. Транзисторы VT2—VT4 могут быть типа КТ3102. Стабилитрон VD15 можно заменить на КС147, КС168, КС170. Пьезокерамический преобразователь ZQ1 — любой. Можно также использовать динамическую головку сопротивлением более 50 Ом, резистор R36 при этом можно из схемы исключить.

Настройка схемы особенностей не имеет. Перед началом работы необходимо настроить детектор на максимальную чувствительность резистором R4. Вращением движка резистора R4 добиваются свечения 1-2 светодиодов и выключения звуковой сигнализации. Прибор готов к работе.

Индикатор напряженности поля на микросхеме К174ПС4

Индикатор напряженности поля представлен на http://cxem.net/indicator/indicator12.php. Для **налаживания** антенно-фидерных трактов любительских радиостанций необходим индикатор напряженности высокочастотного электрического поля. Этот прибор отличается

от обычно используемых высокой чувствительностью и широкой полосой рабочих частот.

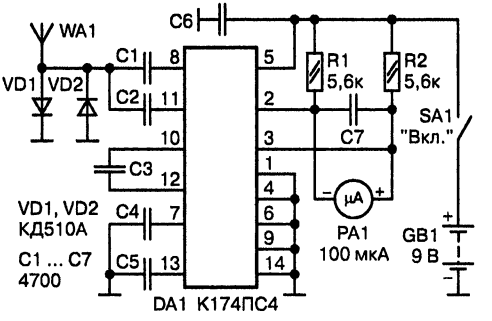


Рис. 7.14. Индикатор напряженности поля

Традиционно индикатор напряженности поля представляет собой антенну (чаще всего, в виде короткого штыря), амплитудный детектор (выпрямитель РЧ напряжений) и стрелочный измеритель (как правило, микроамперметр). Для повышения чувствительности индикатор делают активным, снабжая его усилителем РЧ или постоянного тока. Схема индикатора представлена на **рис. 7.14.**

В индикаторе отсутствует обычный амплитудный детектор, поскольку его функции выполняет микросхема К174ПС4 — перемножитель сигналов, широко используемый радиолюбителями в смесителях радиоприемников, конвертерах и т. д.

В выходном сигнале микросхемы присутствует:

- постоянная составляющая;
- переменная составляющая удвоенной частоты;
- постоянная составляющая пропорциональна квадрату входного напряжения.

Поэтому показания микроамперметра PA1, подключенного к выходу микросхемы, будут пропорциональны мощности сигнала, излучаемой антенной.

Переменную составляющую легко подавить, установив конденсатор C7 достаточной емкости. Диоды VD1, VD2 служат для защиты входных цепей микросхемы от мощных сигналов.

Питается устройство от батареи напряжением 9 В («Крона», «Корунд», «Ника») и потребляет ток примерно 1,5 мА. Работоспособность сохраняется при уменьшении напряжения питания до 6 В. Максимальный ток через микроамперметр PA1 ограничен резисторами R1, R2.

В устройстве можно применить практически любой малогабаритный стрелочный индикатор с током полного отклонения стрелки от 50 до 150 мкА. На частоте 28 МГц чувствительность устройства (минимальный регистрируемый сигнал) был 2—3 мВ, а зависимость показаний от входного напряжения имела квадратичный характер.

Благодаря атому прибор более чувствителен к изменениям напряженности поля, что позволяет точнее настраивать антенно-фидерные

тракты. Так, например, при изменении напряжения на входе устройства в 1,4 раза (3 дБ) показания индикатора увеличиваются вдвое.

Вместо указанной на схеме К174ПС4 допустимо применить микросхемы К174ПС1, К174ПС2. Кроме диодов КД510А, подойдут КД522Б, КД503Б, Конденсаторы — КЛС, КД, К10-17, КМ, резисторы — МЛТ, С2-33, Выключатель — любой малогабаритный, лучше движковый на два положения.

Индикатор поля на базе усилителя постоянного тока на ОУ с каскадом УВЧ и ВЧ детектором

Схема **индикатора поля** (**рис. 7.15**) представляет собой усилитель постоянного тока на ОУ с каскадом УВЧ и ВЧ детектором (http://www.guarda.ru/guarda/data/microwave/txt_08.php).

На входе УВЧ установлен фильтр ВЧ L1, C2, L2, C3, который обрезает сигналы с частотой ниже 10—20 МГц.

Это интересно знать.

В противном случае, прибор начинает реагировать на фон электропроводки и другие индустриальные помехи.

Усилитель ВЧ выполнен по схеме с общим эмиттером, режим выставляется резистором R1 так, что бы на коллекторе VT1 было напряжение равное $U_{кол} = U_{пит}/2$.

Через конденсатор C4 сигнал поступает на диодный детектор VD1. Здесь необходимо применять СВЧ германиевый диод ГД402, ГД507. Но нельзя применять диод Д9, максимальная частота которого 40 МГц.

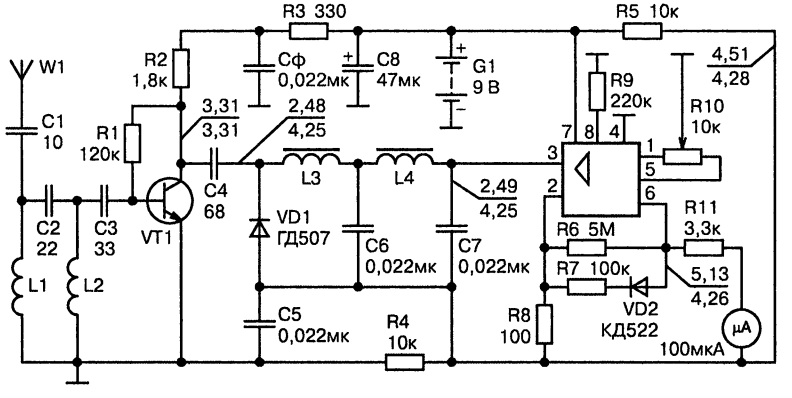


Рис. 7.15. Индикатор поля

Выпрямленный сигнал поступает на вход ОУ через фильтр L3, L4, C6, C7, которые препятствуют попадания на вход ОУ ВЧ составляющей. Операционный усилитель работает от однополярного питания. Поэтому для его нормальной работы при помощи делителя на R4, R5 создана искусственная «средняя точка».

Усиление микросхемы определяется отношением R6/R8 при малых сигналах на входе. При увеличении напряжения на выводе 6 микросхемы до 0,6—0,7 В происходит открывание диода VD2 и в цепь обратной связи усилителя подключается резистор R7, что уменьшает усиление и делает шкалу прибора линейной.

В качестве ОУ можно применить 140УД12 или 140УД6 (предпочтительнее). В случае использования УД6 резистор R9 из схемы необходимо удалить. Резистором R10 осуществляется установка шкалы прибора на 0.

VT1 — СВЧ транзистор, например КТ399.

L1 — 8 витков, провода 0,5 на оправке 5 мм. L2 — 6 витков, того же провода. Дросселя L3, L4 по 60 — 100 мкГн.

Индикатор напряженности поля с пятиуровневой светодиодной шкалой

Индикатор напряженности поля представлен на http://cxem.net/indicator/indicator15.php. Особенность индикатора (**рис. 7.16**) заключается в способе отображения уровня напряженности — на пятиуровневой светодиодной шкале.

Индикатор может контролировать напряженности полей с частотой до 1000 МГц. АЧХ индикатора не измерялось, так как его функция не измерять уровень ВЧ поля в абсолютных значениях, а демонстрировать его уровень и изменение этого уровня в условных единицах.

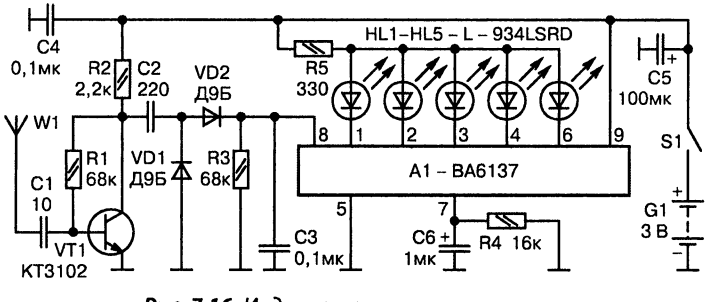


Рис. 7.16. Индикатор напряженности поля

Однако, при наличии необходимой аппаратуры, можно сделать соответствующие таблицы. Во всяком случае, он уверенно реагирует:

- на сигнал СВ-радиостанции, работающей в диапазоне 27 МГц;
- на сигнал сотового телефона, работающего на значительно более высоких частотах.

ВЧ-сигнал наводится в антенне W1 и поступает на усилительный каскад на VT1. Здесь работает относительно низкочастотный транзистор КТ3102. Возможно, используя транзистор типа КТ368, КТ381, можно улучшить работу индикатора на ВЧ. На выходе усилительного каскада включен детектор на германиевых диодах VD1 и VD2.

На конденсаторе С3 выделяется постоянное напряжение, величина которого пропорциональна напряженности ВЧ поля. Это напряжение измеряется шкальным индикатором на поликомпараторной ИМС ВА6137, предназначенной для работы в индикаторах уровня. Уровень напряженности поля оценивают по линейной шкале из пяти светодиодов HL1—HL5.

Индикатор питается от источника из двух последовательно включенных гальванических элементов. Роль корпуса играет пластмассовый футляр для зубной щетки. В нем расположены два элемента питания (один за другим) и детали индикатора. В просверленные отверстия вклеены светодиоды, образующие линейную шкалу. Выводы светодиодов служат и опорными точками для монтажа микросхемы А1.

Роль **антенны** играет складная телескопическая антенна (с поворотным шарниром) радиоприемника или магнитолы. Шарнир закреплен с боковой части корпуса так, что в сложенном положении антенна расположена параллельно корпусу. Для работы ее разворачивают на 180° (или другой угол) и вытягивают на нужную длину. Чувствительность можно регулировать, изменяя длину антенны.

При **налаживании** передатчика индикатор располагают на некотором расстоянии от его антенны, величина которого зависит от мощности и изменение его мощности излучения оценивают при светодиодной шкале. При необходимости индикатор удаляют или приближают к антенне передатчика. Индикатор целесообразно использовать при налаживании передатчиков мощностью не более 0,5 Вт. В противном случае он оказывается слишком чувствительным даже со сложенной антенной и его приходится далеко уносить.

Это интересно знать.

В том случае, если нужно индицировать значительную мощность излучения, можно предусмотреть выключатель, отключающий питание от УВЧ на транзисторе VT1.

Вместо антенны можно подключить объемную катушку диаметром около 100 мм из трех витков толстого намоточного провода. Один конец катушки подключают вместо W1, а второй — на общий минус питания. Не исключен вариант и со сменными перестраиваемыми контурами, на разные частотные участки (получится волномер).

ПОСТАНОВЩИКИ ПОМЕХ РАДИОМИКРОФОНАМ: РАЗРАБОТКА, СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ

В случае, если под рукой нет приемника для поиска радиопередатчиков, но необходимо быть уверенным, что вас не подслушивают, можно воспользоваться передатчиком помех для подавления приемных устройств, которые могут снимать информацию с радиозакладок.

Передатчик помех радиомикрофонам диапазона 100—170 МГц с мощностью излучения около 100 мВт

Сначала рассмотрим схему простого и надежного передатчика помех диапазона 100—170 МГц с мощностью излучения около 100 мВт. Этот диапазон выбран не случайно, так как большинство микропередатчиков предназначены для работы именно в этом диапазоне ввиду наличия дешевых и высококачественных приемников.

Выходная мощность передатчика в пределах 100 мВт позволяет получить на входе расположенного рядом приемникасоотношение «сигнал/шум», 1/100 или 1/50. Этого более чем достаточно даже для экзотических видов модуляции (ЛЧМ,ФКМ и пр.) для того, чтобы полностью подавить информационный сигнал с радиозакладки. Схема передатчика помех для радиозакладок представлена на **рис. 8.1**.

Передатчик помех состоит из двух частей:

- модулятора (выполнен в виде мультивибратора на транзисторах VT1, VT2);
- задающего генератора на транзисторе VT3.

В передатчике помех применена частотная манипуляция с частотой манипуляции 8 Гц и девиацией около 80 кГц (для расширения спектра помехи).

Катушка L1 — бескаркасная, имеет 3—4 витка провода ПЭВ0,8, диаметр катушки 5 мм, шаг намотки 1,5 мм.

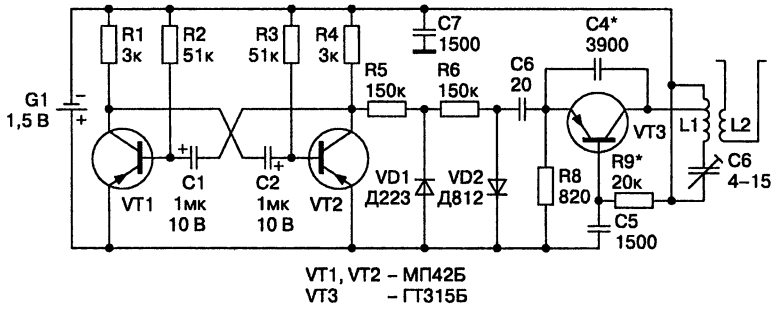


Рис. 8.1. Схема передатчика помех для радиозакладок

Катушка связи L2 — бескаркасная, содержит один виток (диаметром 9 мм) провода ПЭВ-2-0,6 вокруг «холодного» конца катушки L1. Передатчик собран в металлической коробке 40×80 мм. Высокочастотная часть собрана навесным монтажом. В качестве антенны применен полуволновый вибратор из медной проволоки диаметром 2—4 мм.

Простой генератор помех для радиомикрофонов, построенный на микросхеме К174ХА10

Принципиальная схема еще одного **несложного генератора помех** приведена на **рис. 8.2**. Источником шума является полупроводниковый диод — стабилитрон VD1 типа КС168А, работающий в режиме лавинного пробоя при очень малом токе. Сила тока через стабилитрон VD1 составляет всего лишь около 100 мкА. Шум, как полезный сигнал, снимается с катода стабилитрона VD1и через конденсатор С1 поступает на инвертирующий вход операционного усилителя DA1 типа КР140УД1208. На неинвертирующий вход этого усилителя посту-

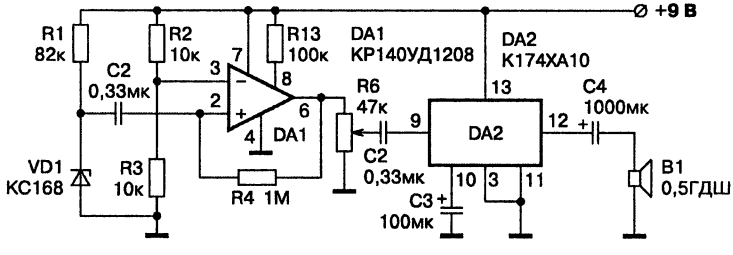


Рис. 8.2. Принципиальная схема несложного генератора помех

пает напряжение смещения, равное половине напряжения питания с делителя напряжения, выполненного на резисторах R2 и R3.

Режим работы микросхемы определяется резистором R5, а коэффициент усиления — резистором R4. С нагрузки усилителя, переменного резистора R6, усиленное напряжение шума поступает на усилитель мощности, выполненный на микросхеме DA2 типа К174ХА10. С выхода усилителя шумовой сигнал через конденсатор С4 поступает на малогабаритный широкополосный громкоговоритель В1.

Уровень шума регулируется резистором R6. Стабилитрон VD1 генерирует шум в широком диапазоне частот от единиц герц до десятков мегагерц. Однако на практике он ограничен АЧХ усилителя и громкоговорителя.

Стабилитрон VD1 подбирается по максимальному уровню шума, но так как стабилитроны представляют собой некалиброванный источник шума, то стабилитрон может быть любым, с напряжением стабилизации менее напряжения питания.

Микросхему DA1 можно заменить микросхемой КР1407УД2 или использовать любой операционный усилитель с высокой граничной частотой коэффициента единичного усиления. Вместо усилителя на DA2 можно использовать любой другой УЗЧ. Подробнее схема широко рассмотрена в интернете, например, на http://leg ion-33/Sxemy/G_belogo_huma.htm.

Простой генератор помех радиомикрофонам на ИМС 74LS04 с рабочим диапазоном 500 МГц

Предлагаемая схема генератора помех на ИМС 74LS04 очень проста. Но, тем не менее, она эффективно глушит диапазон примерно в 500 МГц на расстоянии до 30 м. Устройство (**рис. 8.3**) выполнено на одной микросхеме 74LS04 (можно также использовать К555ЛН1, КР1533ЛН1, КР531ЛН1), и подстроечном конденсаторе емкостью 3—15 пФ.

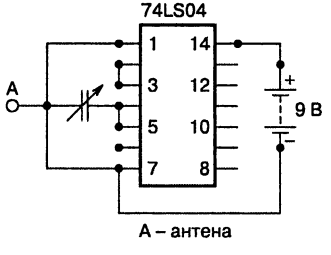


Рис. 8.3. Схема генератора помех на ИМС 74LS04

В качестве антенны использован кусок провода длинной 20—30 см. В зависимости от емкости конденсатора можно перестроиться на любую полосу частот шириной в 500 МГц.

Мощный генератор помех на биполярном транзисторе КТ904А

Мощный генератор помех (рис. 8.4) основан на распространенной сейчас в Интернете схеме передатчика на 10 Вт, предложенной М. Анисимовым.

Катушки имеют следующие параметры:

- L1 — 4 витка ПЭВ-1,0 на оправке 12 мм, отвод от середины;
- L2 — дроссель 20 мкГн, подходит от китайского приемника;
- L3 — 8 витков ПЭВ-1,0 на оправке 8 мм, намотана на оболочке кабеля РК-75;
- L4 — 6 витков того же провода и на той же оправке, расположена между 2-х половин L3.

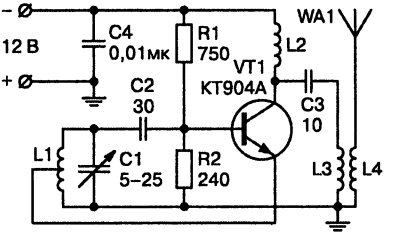


Рис. 8.4. Принципиальная схема мощного генератора помех

Следует отметить, что батарейное питание тут не эффективно, ток потребления устройства более 0,5 А, поэтому нужен хороший блок питания. Транзистор должен стоять на хорошем радиаторе, иначе он может просто сгореть. Антенной служит штырь длиной 1 м. Генератор помех начинает работать сразу и настройки не требует.

Описание устройства приводится на http://www.general.pop3.ru/generato.gif.

Генератор подавления маломощных передатчиков диапазона 30—1000 МГц

Генератор подавления радиопередатчиков рассматривается на http://isinpol.net/radio-master/10-generator-podavleniya-radioperedatchikov.html. Этот постановщик радиопомех предназначен для работы в системе активной зашиты информации. Постановщик радиопомех во включенном состоянии создает электромагнитные помехи в эфире с интенсивностью, достаточной для маскирования информативных излучений от используемой оргтехники, в том числе от ПК. Генератор также обеспечивает эффективное подавление излучений маломощных передатчиков диапазона 30—1000 МГц.

Данная модификация прибора, кроме того, может применяться для предотвращения активации радиомикрофонов с дистанционным

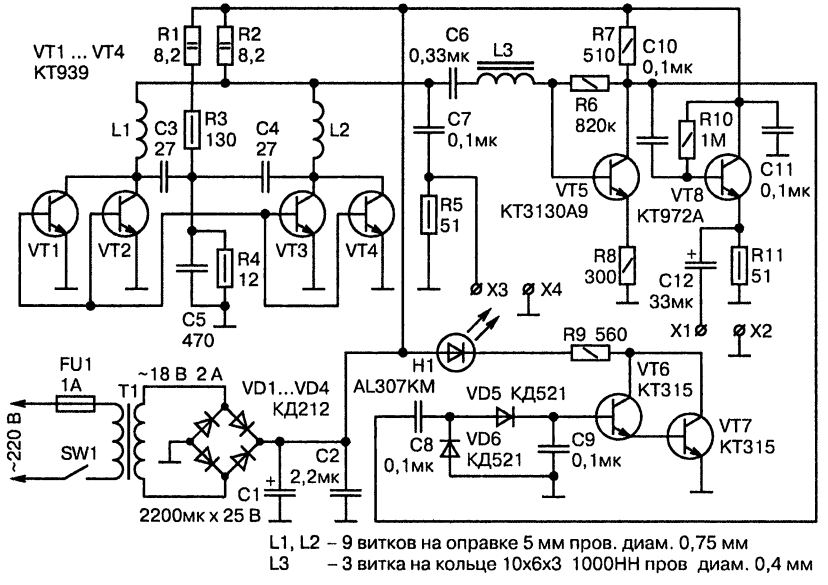


Рис. 8.5. Генератор подавления радиопередатчиков

управлением, посредством воздействия на входные цепи приемника дистанционного управления.

Генератор (**рис. 8.5**) построен по классической схеме шумового генератора радиочастотного диапазона. Однако следует отметить, что тепловой режим работы схемы очень тяжелый. На транзисторы VT1—VT4 необходимы радиаторы не менее 100 см^2 на каждый, при условии хорошей внутренней вентиляции корпуса. Резисторы R1 и R2 лучше заменить на один 4,7 Ом мощностью 10 Вт.

Стабилизированный генератор шума

Стабилизированный генератор шума рассматривается на http://www.cqham.ru/hpa14.htm. Благодаря простоте схемы и удобству градуировки генераторы шума на прямонакальных диодах получили широкое распространение среди радиолюбителей.

При всех достоинствах схемы существует один **недостаток**, делающий работу с ними не совсем приятной, а именно — крайнее неудобство установки и поддержания низких уровней шума, соответствующих токам через диод порядка единиц миллиампер.

Проблема возникает из-за резкой нелинейности зависимости тока анода диода от напряжения накала. Это затрудняет регулировку анод-

ного тока с помощью стабилизатора с низким выходным сопротивлением. Применение для этих целей реостата тоже не очень хорошее решение из-за скачков тока при перестройке и большой нелинейности регулировочной характеристики.

Можно ли создать генератор шума, в котором регулировка выходной мощности осуществляется линейно, в любом диапазоне и поддерживается на заданном уровне при изменении сетевого напряжения? Да, и это не сложно.

Идея состоит в том, что нить накала диода питается от стабилизатора, охваченного обратной связью не по своему выходу, а по току анода. Петля обратной связи замыкается через промежуток катод-анод диода. При этом зависимость тока анода от напряжения накала диода, включенного в цепь обратной связи, линеаризуется пропорционально коэффициенту усиления в петле, который можно сделать очень высоким.

Ниже приведена схема, реализующая этот принцип (**рис. 8.6**).

Сам генератор шума выполнен на диоде V1. Показанное на схеме включение диода позволяет избавиться от дросселя в анодной цепи. Это улучшает частотную характеристику прибора на УКВ. Но при этом требуется перенос регулирующего элемента к высокопотенциальному концу анодного источника.

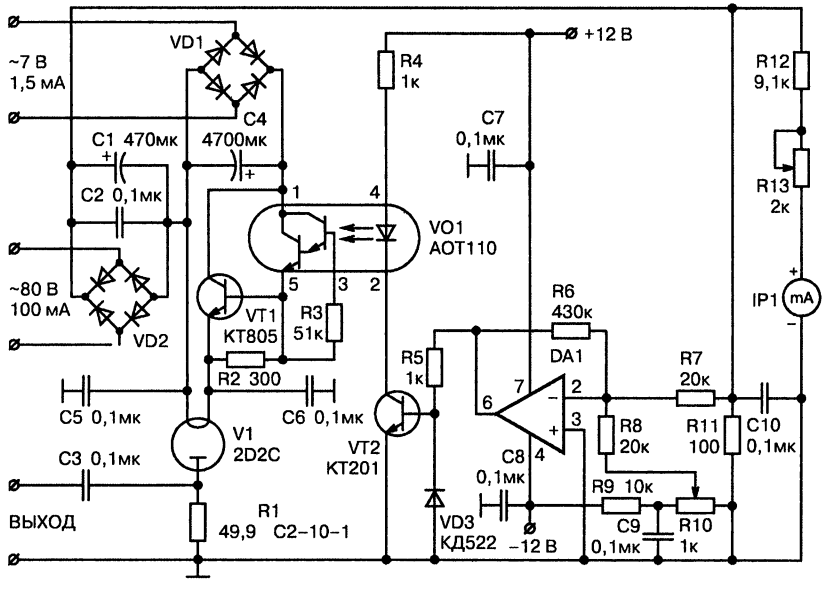


Рис. 8.6. *Стабилизированный генератор шума*

Источник питания нити накала собран на диодном мосте VD1 и конденсаторе C4. Напряжение с этого источника подается на нить накала диода через регулирующий транзистор VT1. Оптрон VO1, управляющий транзистором VT1, предназначен для сдвига тока управления «вверх».

Источник питания анода выполнен на диодном мосте VD2 и конденсаторах C1 и C2. Напряжение, пропорциональное току анода диода, выделяется относительно общего провода на шунте R11. На операционном усилителе DA1 выполнена схема, вырабатывающая напряжение, пропорциональное разности сигналов с шунта R11 и задатчика тока анода — резистора R10.

Выходное напряжение ошибки через транзистор VT2 управляет током оптрона VO1, и, следовательно, напряжением на нити накала диода. При этом напряжение на шунте R11 стремится стать равным напряжению на движке резистора R10.

Это интересно знать.

В такой схеме значение тока анода определяется только напряжением на движке задатчика R10 и не зависит от прогрева диода, нестабильности питающей сети и прочих дестабилизирующих фактов.

Номиналы резисторов на приведенной схеме соответствуют диапазону регулировки тока анода от 0 до 10 мА. При необходимости диапазон можно сделать любым. Можно переключать его в необходимых пределах. Для этого нужно всего-навсего изменить сопротивление шунта R11 таким образом, чтобы при максимальном требуемом токе анода падение напряжения на нем соответствовало максимальному напряжению задатчика (т. е. 1 В).

Например, для получения диапазона 0—5 мА сопротивление шунта R11 должно быть 200 Ом. При больших значениях сопротивления шунта во время настройки необходимо учитывать влияние тока через головку IP1 (100 мкА), измеряющую уровень шума на выходе.

Будьте осторожны.

Следует учесть, что из-за наличия инерционного элемента в цепи обратной связи (нить накала) в схеме возможны автоколебания.

На стабильности выходного тока это абсолютно не сказывается. Однако если автоколебания присутствуют (что можно увидеть осциллографом на

выходе DA1),можно при желании попытаться их ликвидировать, уменьшая усиление в петле ОС (уменьшить номинал резистора R6).

Напряжения питания операционного усилителя (любой тип современного ОУ с соответствующими цепями коррекции) должно быть стабилизировано, т. к. с него формируется опорное напряжение задатчика.

При необходимости можно проградуировать ручку задатчика линейно прямо в единицах тока и отказаться от измерительного прибора.

В цепь накала рекомендуется включить полисвич на 1—1,5 А для защиты нити накала при настройке схемы или при выходе из строя компонентов схемы.

Генератор шума на трех КМОП микросхемах для защиты от снятия информации с оконного стекла

Генератор шума рассмотрен на http://cxem.net/guard/3-10.php. Существуют специальные приборы, которые позволяют на расстоянии прослушивать разговоры через оконные стекла. При этом используется свойство звуковых волн создавать микровибрацию стекла, которую с помощью узконаправленных оптических приборов можно преобразовать в звук.

Предотвратить прослушивание деловых разговоров через окна позволяет генератор широкополосного акустического шума (**рис. 8.7**).

Устройство собрано на трех КМОП микросхемах и состоит из задающего генератора на частоту 50 кГц (D1.1, D1.2), формирователя псевдослучайной последовательности импульсов на сдвигающих регистрах (D2, D3) и логике (D1.3, D1.4).

Звуковыми излучателями (HF1, HF2) являются телефонные капсули ВП-1 или ДЭМ-4М.

Резистор R4 позволяет регулировать громкость звука.

Схема может питаться от любого нестабилизированного источника с напряжением от 4 до 15 В и потребляет ток не более 20 мА.

В качестве источника звука подойдут и любые малогабаритные динамики (с 50-омным сопротивлением), но при этом возрастет потребляемый ток. Транзисторы можно заменить на КТ829А.

При правильной сборке схема **настройки не требует**. Устройство выполняется в виде переносной коробки и размещается на подоконнике, вблизи от стекла. Включать генератор шума можно при проведении деловых переговоров, в случае необходимости.

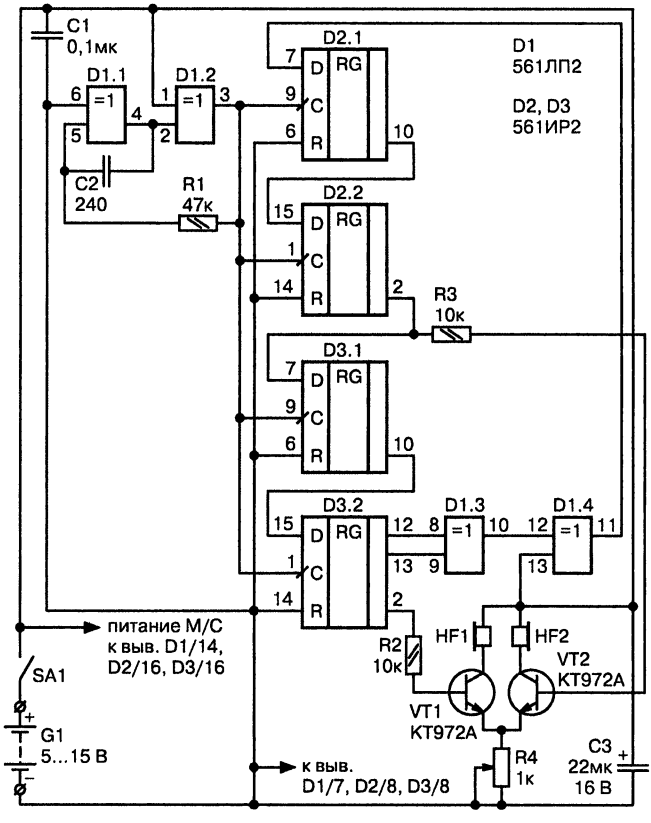


Рис. 8.7. Генератор шума

Широкополосный генератор шума на биполярных транзисторах

Широкополосный генератор шума рассматривается на http://mods.radioscanner.ru/selfmade/mod338/. Электрическая схема такого широкополосного генератора шума приведена на **рис. 8.8**. Собственно источником шума в ней служит стабилитрон VD2, на транзисторе VT1 выполнен широкополосный усилитель шумового напряжения, а на транзисторе VT2 — эмиттерный повторитель для согласования генератора с 50-омной нагрузкой.

В отличие от других схем генератора шума, источник шума на стабилитроне VD2 в этой схеме включен не в цепь базы транзистора VT1, а в цепь эмиттера. База транзистора VT1 по переменному току соединена с общим проводом схемы конденсаторами C1 и C2. Таким образом, транзистор VT1 в усилительном каскаде включен по схеме с

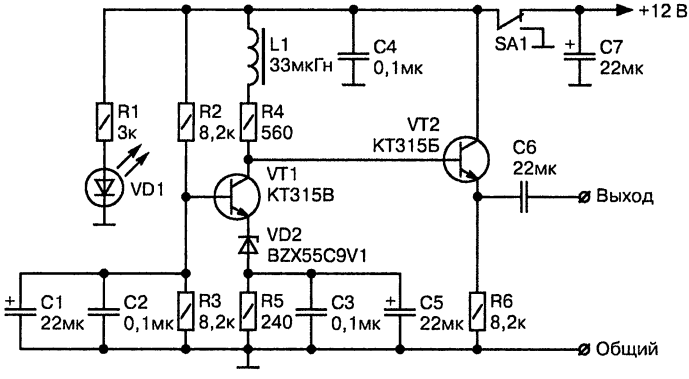


Рис. 8.8. Широкополосный генератор шума

общей базой. Поскольку схема с общей базой лишена главного недостатка схемы с общим эмиттером — эффекта Миллера, то такое включение обеспечивает максимальную широкополосность усилителя шумового напряжения для данного типа транзистора.

А такой недостаток схемы с общей базой, как высокое выходное сопротивление, компенсируется затем эмиттерным повторителем на транзисторе VT2. В итоге выходное сопротивление генератора шума составляет около 50 Ом (более точно устанавливается подбором резистора R6).

Режимы работы транзисторов VT1, VT2 и стабилитрона VD2 по постоянному току устанавливаются резисторами R2, R3 и R5:

- напряжение на базе транзистора VT1, равное половине напряжения питания, устанавливается состоящим из двух одинаковых резисторов R1 и R2 делителем напряжения;
- ток через стабилитрон VD2 устанавливается резистором R5.

Нижний по схеме вывод стабилитрона VD2 по переменному току соединен с общим проводом схемы конденсаторами C3 и C5. Дроссель L1 несколько поднимает усиление по напряжению усилителя на транзисторе VT1 и тем самым в некоторой степени компенсирует падение уровня шумового сигнала на частотах выше 2 МГц. Светодиод VD1 служит для индикации включения питания генератора шума выключателем SA1.

Цифровой генератор шума

Цифровой генератор шума представлена на http://newsrack.ru/content/view/472/25/. Цифровой шум представляет собой временной слу-

чайный процесс, близкий по своим свойствам к процессу физических шумов. Поэтому он называется **псевдослучайным процессом**. Цифровая последовательность двоичных символов в цифровых генераторах шума называется псевдослучайной последовательностью и представляет собой последовательность прямоугольных импульсов псевдослучайной длительности с псевдослучайными интервалами между ними.

Период повторения всей последовательности значительно превышает наибольший интервал между отдельными импульсами последовательности.

Наиболее часто в цифровых генераторах шума применяются последовательности максимальной длины — так называемые М-последовательности, которые формируются при помощи регистров сдвига и сумматоров по модулю 2, использующихся для получения сигнала обратной связи.

Принципиальная схема генератора шума с равномерной спектральной плотностью в рабочем диапазоне частот приведена на **рис. 8.9**.

Этот генератор шума содержит:

- последовательный восьмиразрядный регистр сдвига, выполненный на микросхеме К561ИР2;
- сумматор по модулю 2 (DD2.1);
- тактовый генератор (DD2.3, DD2.4);
- цепь запуска (DD2.2).

Последние элементы выполнены на микросхеме К561ЛП2. Тактовый генератор выполнен на элементах DD2.3 и DD2.4 по схеме мультивибратора. С выхода генератора последовательность прямоугольных импульсов с частотой следования около 100 кГц поступает на входы «С» регистров сдвига DD1.1 и DD1.2, образующих 8- разрядный регистр сдвига.

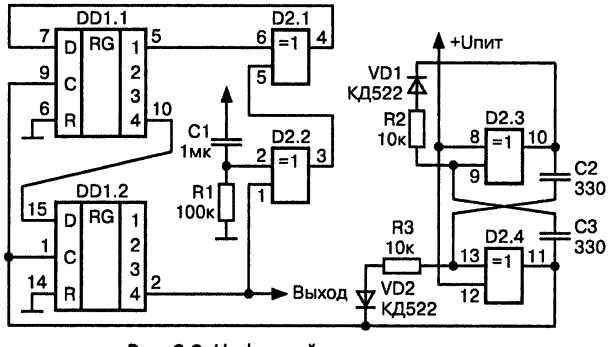


Рис. 8.9. Цифровой генератор шума

Запись информации в регистр происходит по входам «D». На вход «D» регистра DD1.1 сигнал поступает с элемента обратной связи — сумматора по модулю 2 на элементе DD2.1. Однако при включении питания возможно состояние регистров, когда на всех выходах присутствуют низкие уровни.

Так как в регистрах М-последовательности запрещено появление нулевой комбинации, то в схему введена специальная цепь запуска генератора, выполненная на элементе DD2.2. При включении питания он формирует на своем выходе уровень логической единицы, который выводит регистр из нулевого состояния. Затем на дальнейшую работу генератора цепь запуска не оказывает никакого влияния. Сформированный псевдослучайный сигнал снимается с 8-го разряда регистра сдвига и поступает для дальнейшего усиления и излучения. Напряжение источника питания может быть от 3 до 15 В.

В устройстве использованы КМОП микросхемы серии 561, их можно заменить микросхемами серий К564, К1561 или К176. В последнем случае напряжение питания должно быть 9 В.

Правильно собранный генератор в налаживании не нуждается. Изменением тактовой частоты генератора можно регулировать диапазон частот шума и интервал между спектральными составляющими.

СНЯТИЕ ИНФОРМАЦИИ СО СТЕКЛА И ПРОТИВОДЕЙСТВИЕ СНЯТИЮ

*Из главы 6 стало понятно, что собрать «**жучок**» совсем несложно. Однако и обнаружить такие радиомикрофоны можно без особого труда, стоит только применить **детектор поля**, рассмотренный выше.*

*Вместе с тем, существует принципиально **иной способ снятия информации**. С оконного стекла!*

Лазерные средства акустической разведки

В последние годы появилась информация, что спецслужбы различных стран для несанкционированного получения речевой информации все чаще используют дистанционные **портативные средства акустической разведки**.

Самыми современными и эффективными считаются **лазерные системы акустической разведки**, которые позволяют воспроизводить речь, любые другие звуки и акустические шумы при лазерно-локационном зондировании оконных стекол и других отражающих поверхностей.

По свидетельству прессы (в том числе и специальных изданий), в США, например, в середине 80-х годов продавцы спецтехники отметили всплеск интереса у покупателей именно к **лазерным микрофонам**. Не меньший интерес в настоящее время проявляется к данным изделиям и в России (http://bezpeka.desant.com.ua).

На сегодняшний день создано целое семейство **лазерных средств акустической разведки**. В качестве примера можно привести систему SIPE LASER 3-DA SUPER. Данная модель состоит из следующих компонентов:

- источника излучения (гелий-неоновый лазер);
- приемника этого излучения с блоком фильтрации шумов;
- двух пар головных телефонов;
- аккумулятора питания и штатива.

Работает эта система так. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Изменять угол расходимости выходящего. пучка позволяет оптическая насадка, высокая стабильность параметров достигается благодаря использованию системы автоматического регулирования. Модель обеспечивает съем речевой информации с оконных рам с двойными стеклами с хорошим качеством на расстоянии до 250 м.

Физические основы перехвата речи лазерными микрофонами

Рассмотрим кратко физические процессы, происходящие при перехвате речи с помощью лазерного микрофона. Зондируемый объект — обычно оконное стекло — представляет собой своеобразную **мембрану**, которая колеблется со звуковой частотой, создавая фонограмму разговора.

Генерируемое лазерным передатчиком излучение, распространяясь в атмосфере, отражается от поверхности оконного стекла и модулируется акустическим сигналом, а затем воспринимается фотоприёмником, который и восстанавливает разведываемый сигнал.

В данной технологии принципиальное значение имеет **процесс модуляции.** Звуковая волна, генерируемая источником акустического сигнала, падает на границу раздела воздух-стекло и создает своего рода вибрацию, то есть отклонения поверхности стекла от исходного положения. Эти отклонения вызывают **дифракцию света**, отражающегося от границы.

Если размеры падающего оптического пучка малы по сравнению с длиной «поверхностной» волны, то в суперпозиции различных компонент отраженного света будет доминировать дифракционный пучок нулевого порядка:

- во-первых, фаза световой волны оказывается промодулированной по времени с частотой звука и однородной по сечению пучка;
- во-вторых, пучок «качается» с частотой звука вокруг направления зеркального отражения.

На качество принимаемой информации оказывают влияние следующие факторы:

- параметры используемого лазера (длина волны, мощность, когерентность и т. д.);
- параметры фотоприемника (чувствительность и избирательность фотодетектора, вид обработки принимаемого сигнала);
- наличие на окнах защитной пленки;

Это интересно знать.
При установке слоя защитной и слоя тонирующей пленки значительно снижается уровень вибрации стекла, вызываемой акустическими (звуковыми) волнами. Снаружи трудно зафиксировать колебания стекла, поэтому трудно выделить звуковой сигнал в принятом лазерном излучении.

- параметры атмосферы (рассеяние, поглощение, турбулентность, уровень фоновой засветки и т. д.);
- качество обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды — грязь, царапины);
- уровень фоновых акустических шумов;
- уровень перехваченного речевого сигнала; конкретные местные условия.

Это интересно знать.
Все эти обстоятельства накладывают свой отпечаток на качество фиксируемой речи, поэтому нельзя принимать на веру данные о приеме с дальности в сотни метров — эти цифры получены в условиях полигона, а то и расчетным путем.

Из всего вышесказанного можно сделать следующие **выводы**:
- лазерные системы съема существуют и являются при грамотной эксплуатации весьма эффективным средством получения информации;
- лазерные микрофоны не является универсальным средством, так как многое зависит от условий применения;
- не все то является лазерной системой разведки, что так называется продавцом или производителем;
- без квалифицированного персонала тысячи и даже десятки тысяч долларов, потраченные на приобретение лазерного микрофона, пропадут зря;
- службы безопасности должны разумно оценить необходимость защиты информации от лазерных микрофонов.

Принцип работы лазерного микрофона представлен на **рис. 9.1**. А на **рис. 9.2** показаны объективы оптического передатчика и оптического приемника ЛСАР.

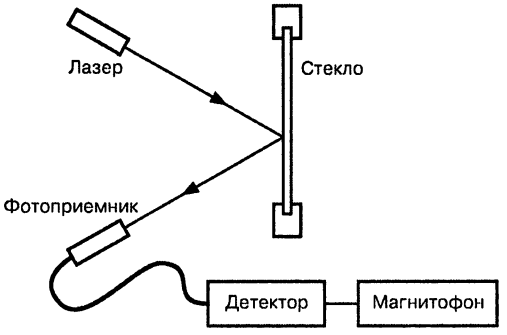


Рис. 9.1. Принцип работы лазерного микрофона

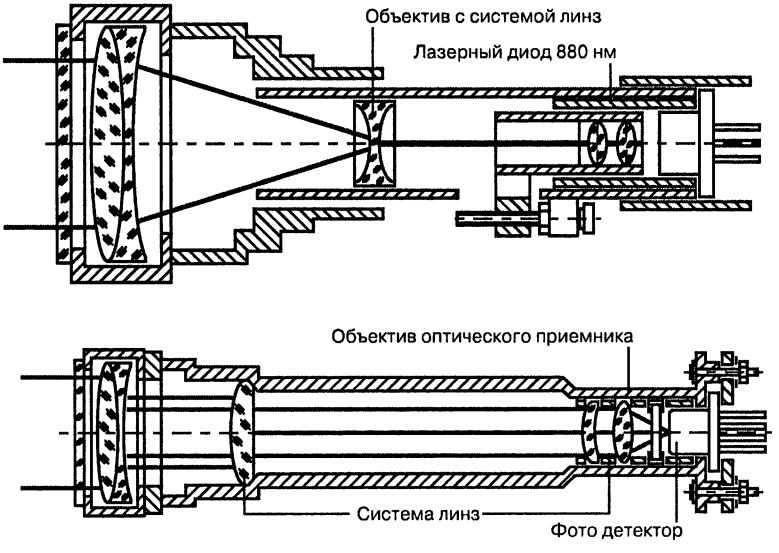


Рис. 9.2. Объективы оптического передатчика и оптического приемника ЛСАР

Защита от лазерного микрофона своими руками: устанавливаем схему, модулирующую оконное стекло

Но даже лазерному детектору можно поставить помеху. На **рис. 9.3** показана схема, модулирующая стекло.

Резонирующим элементом служит **пьезоэлемент**, который жестко крепится по центру стекла для обеспечения максимальной амплитуды. Схема собрана на ТТЛ микросхемах, потребляющих большой ток, поэтому для питания необходимо использовать сетевой блок питания.

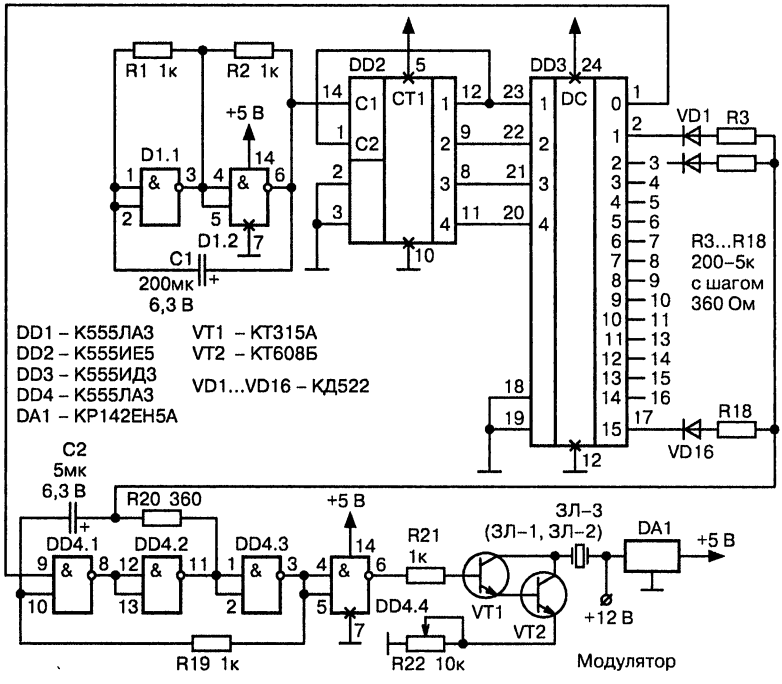


Рис. 9.3. *Модулятор оконного стекла*

Пьезодатчик модулирует стекло таким образом, что амплитуда модуляции стекла выше, чем модуляция голосом при средней громкости произношения. Кроме того, пьезоэлемент модулирует стекло на разных частотах, что еще больше затрудняет съем информации через стекло.

Защита от лазерного микрофона своими руками: устанавливаем простую схему модуляции оконного стекла на реле

Существует и более простая схема срыва прослушивания (**рис. 9.4**).

В качестве модулятора с частотой 50 Гц используется обычное малогабаритное реле постоянного тока РЭС 22, РЭС 9. Выводы обмотки подключаются к переменному току напряжением чуть ниже порога срабатывания. Реле жестко крепится к стеклу клеем ЭПД. Так же можно попробовать совсем элементарную схему для защиты от ЛСАР.

Это интересно знать.

Все мы знаем закон физики — «Угол падения равен углу отражения». Это значит, что надо находиться строго перпендикулярно окну прослушиваемого помещения. Из квартиры напротив вы вряд ли поймаете отраженный луч, так как стены здания обычно, я уж не говорю об окнах, немного кривоваты и отраженный луч пройдет мимо.

Перед важным совещанием приоткройте окно, и пока шпионы бегают по соседним зданиям и ищут отраженный луч, вы, наверняка, успеете обсудить все важные моменты, а если менять положение окна каждые 5—10 мин. (приоткрыть, закрыть), то все желание прослушивать вас после такого марафона пройдет.

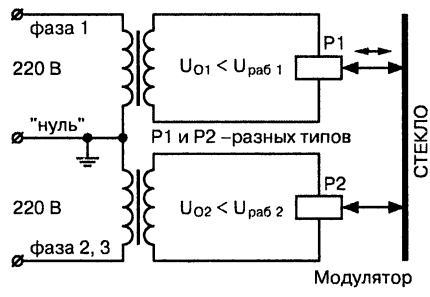


Рис. 9.4. Схема срыва прослушивания

Проблема противодействия съему информации с использованием лазерного излучения остается весьма актуальной и в то же время одной из наименее изученных по сравнению с другими, менее «экзотическими» средствами промышленного шпионажа.

Особая привлекательность таких систем обусловлена тем, что они позволяют решать задачи съема речевой информации максимально безопасно, на расстоянии. Снимается необходимость захода в интересующее помещение с целью размещения там подслушивающего устройства, что всегда связано с риском. Кроме того, и выявление работающего лазерного микрофона очень сложно, а в ряде случаев технически неосуществимо.

Использование ИК-диапазона для снятия информации с оконного стекла

Внимание.

Использование этих устройств в некоторых случаях запрещено законодательством РФ и может привести к административной или уголовной ответственности.

Выше отмечалось, что звуковые волны в помещении вызывают микровибрации оконных стекол. Но на окно можно направить не

только лазерный луч (что очень дорого, десятки тысяч долларов стоит лазерный микрофон), но и поток ИК-излучения. И в этом случае большая часть ИК-излучения пройдет через стекло внутрь, однако будет и отражение. При этом отраженный поток окажется промодулированным речевой информацией. Такую систему может создать и радиолюбитель.

Устройство стоит из двух относительно независимых частей: ИК-передатчика; ИК-приемника.

Принципиальная **схема ИК-передатчика** показана на **рис. 9.5, *а***. В приведенном на **рис. 9.5, *б*** варианте схема с К1401УД4 обеспечивала уверенный съем информации с расстояния 5—10 м, вариант с TLE2074CN обеспечивал съем информации с расстояния до 15—20 м. Кроме того, второй вариант в силу более низкого уровня шумов позволял уверенно разбирать тихие слова даже на фоне громкой музыки.

Рассмотрим **передатчик**. Основу передатчика составляет генератор прямоугольных импульсов на микросхеме D1. Выходной сигнал генератора с частотой 35 кГц поступает на базу транзистора VT1, который совместно с VT2 образует составной транзистор. При помощи этого транзистора коммутируется ИК-светодиод VD1.

Отраженный сигнал поступает на вход приемника, схема которого показана на **рис. 9.5, *б***. Принятый фотодиодом VD1 сигнал поступает на вход усилителя, собранного на ОУ A1.1.

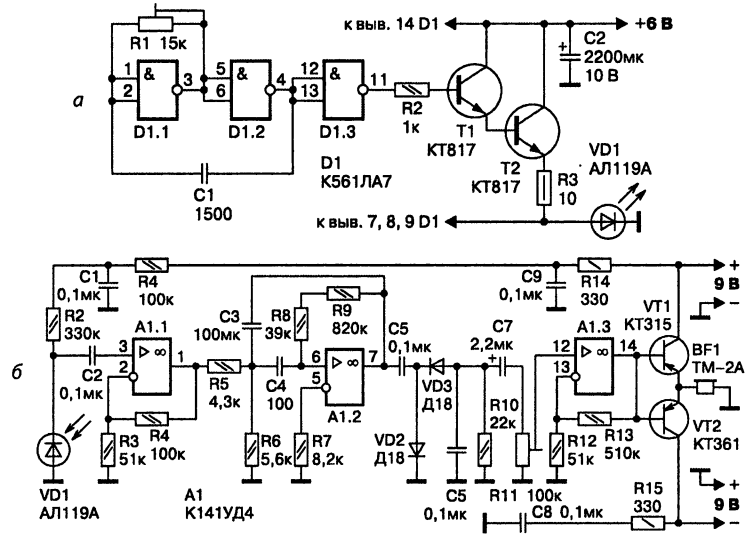


Рис. 9.5. *Устройство для снятия информации со стекла по ИК-каналу: а — схема ИК-передатчика; б — схема ИК-приемника*

Здесь вся полоса принятых частот усиливается в два раза, а также обеспечивается согласование фотодиода с последующими каскадами. На ОУ A1.2 собран активный полосовой фильтр, настроенный на частоту 34,67 кГц, т. е. на частоту несущей передатчика.

Коэффициент усиления каскада равен 100, полоса пропускания с неравномерностью 3 дб — 6,8 кГц, это обеспечивает избирательное усиление несущей и боковых полос. Такое построение схемы позволяет максимально ослабить действие помех и паразитного фона от осветительных приборов.

С выхода A1.2 сигнал поступает на амплитудный детектор, построенный по классической схеме, не требующей пояснений. На ОУ A1.3 и транзисторах VT1 и VT2 построен УНЧ, нагрузкой которого служат высокоомные телефоны ТМ-2А или аналогичные. Развязка узлов схемы по питанию осуществляется цепями R1 C1, R14 C9, R15 C8.

Наладка правильно собранной схемы сводится к подстройке частоты передатчика резистором R1 до получения на выходе приемника максимальной амплитуды сигнала. ОУ К1401УД4 не имеет прямой замены среди отечественных микросхем, но вместо A1.1 и A1.2 можно применить любые ОУ с полевыми транзисторами на входе и частотой единичного усиления не менее 2,5 МГц. A1.3 можно заменить на любой ОУ широкого применения.

Во время испытаний устройства проверялся такой вариант: КР574УД2Б и К140УД708. Заметно повысить характеристики приемника можно, если применить малошумящие ОУ TLE2074CN и TLE2144CN фирмы Texas Instruments.

Цоколевка этих микросхем полностью совпадает с цоколевкой К1401УД4. Светодиод и фотодиод можно взять зарубежного производства от систем ДУ телевизоров.

Это интересно знать.

Чувствительность устройства можно повысить дополнительными ИК-светодиодами, включенными параллельно VD1 передатчика (через свои ограничительные резисторы). Можно также увеличить коэффициент усиления приемника, добавив каскад, аналогичный каскаду на A1.2. Для этого можно использовать свободный ОУ микросхемы A1.

Конструктивно светодиод и фотодиод расположены так, чтобы исключить прямое попадание ИК-излучения светодиода на фотодиод, но уверенно принимать отраженное излучение.

Питание приемника осуществляется от двух батареек типа «Крона», передатчик питается от четырех элементов типа R20 суммарным напряжением 6 В (1,5 В каждый).

В инфракрасных устройствах с передачей и приемом луча приемник и передатчик принято выполнять **автономными блоками**, хотя в большинстве случаев они, как минимум, имеют общий источник питания, а то и расположены рядом друг с другом (http://microcopied.ru/content/view/475/25/1/0/).

Поэтому если к двум проводам, идущим к приемнику от общего с передатчиком источника питания, прибавить всего один провод синхронизации, то можно получить замечательное устройство. Оно будет работать по принципу синхронного детектора и обладать такими его свойствами, как:

- избирательность;
- помехоустойчивость;
- возможность получения большого усиления.

И это без применения многокаскадных усилителей со сложными фильтрами.

Внутри помещения даже без использования дополнительной оптики и мощных излучателей устройство можно применять как охранную сигнализацию, срабатывающую при пересечении инфракрасного луча на расстоянии от излучателя до приемника 3—7 м.

Причем устройство не реагирует на внешнюю засветку от посторонних источников, как постоянную (солнце, лампы накаливания), так и модулируемую (люминесцентное освещение, фонарик).

Снабдив светодиод приемника **собирающей линзой**, можно перекрыть несколько десятков метров расстояния на открытом пространстве, имея отличную помехоустойчивость даже при идущем слабом снеге. При использовании линз на приемнике и передатчике одновременно возможно перекрытие еще большего расстояния, но возникает проблема точного наведения узкого луча передатчика на линзу приемника.

Генератор передатчика (рис. 9.6) собран на интегральном таймере DA1 включенном по схеме мультивибратора. Частота мультивибратора выбрана в диапазоне 20—40 кГц, но может быть любой. Она лишь

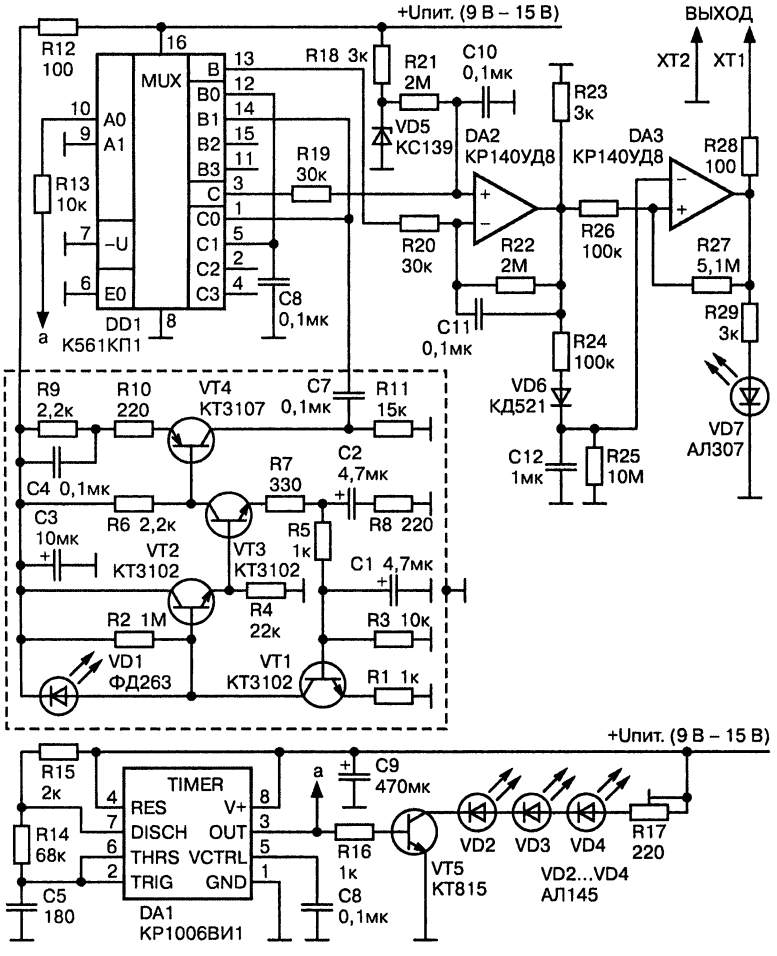


Рис. 9.6. Схема передатчика

ограничена снизу величиной конденсаторов С7, С8 и сверху частотными свойствами таймера.

Сигнал мультивибратора через ключ на VT5 управляет светодиодами передатчика VD2—VD4. Мощность излучения передатчика можно подбирать, меняя число светодиодов или ток через них резистором R17. Так как диоды работают в импульсном режиме, амплитудное значение тока через них можно выставить вдвое-втрое выше постоянно допустимого.

Инфракрасный приемник (рис. 9.7) выполнен на дискретных элементах VD1, VT1—VT4, Rl—R12, C1—C4 по схеме, использовав-

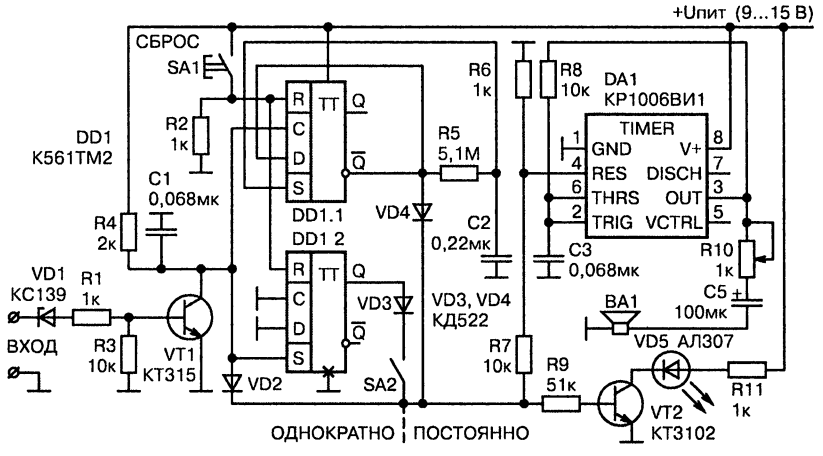


Рис. 9.7. *Схема приемника*

шейся во многих советских телевизорах. Его с успехом можно заменить импортным интегральным ИК-приемником, имеющим к тому же инфракрасный светофильтр. Однако желательно, чтобы на выходе приемника не формировался цифровой сигнал, то есть его тракт был бы линейным.

Далее усиленный сигнал поступает на **синхронный детектор**, выполненный на КМОП мультиплексоре DD1 и управляемый сигналом таймера DA1. На выходах 3, 13 DD1 имеется полезный противофазный сигнал, который усиливается дифференциальным интегратором на ОУ DA2. Элементы R19, R20; C10, C11; R21, R22 интегратора определяют уровень усиления сигнала, полосу пропускания приемника и скорость отклика.

Это интересно знать.

Для достижения максимальной помехоустойчивости и уровня усиления желательно, чтобы эти элементы были попарно подобраны с точностью до 1%.

Уровень «земли» интегратора определяется стабилитроном VD5, и выбран как можно меньшим, (но чтобы ОУ DA2 не входил в ограничение), так как полезный сигнал на выходе DA2 будет положительным.

На ОУ DA3 выполнен триггер Шмитта. Совместно с пиковым детектором на элементах R24, VD6, R25, C12 он исполняет роль компаратора для формирования сигнала срабатывания. Падение напряжения

на диоде VD6 уменьшает уровень пикового напряжения на величину 0,4—0,5 В. Это задает «плавающий» порог срабатывания сигнализации, величина которого плавно меняется в зависимости от расстояния между приемником и передатчиком, уровня засветок, помех. При нормальном прохождении луча светодиод VD7 будет светиться, при пересечении луча светодиод гаснет.

К **деталям**, применяемым в схеме, никаких особых требований нет. Элементы могут быть заменены аналогичными импортными или отечественными. Резистор R25 составлен из двух последовательных по 5,1 МОм. Фотодиод VD1 с усилителем обязательно должен быть помещен в металлический заземленный экран для предотвращения наводок.

Схема настройки не требует, но следует быть внимательным при испытании устройства. Сигнал передатчика может попадать в приемник в результате отражения от близлежащих предметов и не даст увидеть результат функционирования схемы. Удобнее всего во время отладки уменьшить ток свето-диодов излучателя до долей миллиампера.

Для работы устройства в качестве ИК сигнализации работающей на пересечение луча к устройству (**рис. 9.6**) можно подключить блок индикации (**рис. 9.7**). Переключателем SA2 выбирается режим работы блока индикации. В положении «ОДНОКРАТНО» при пересечении луча формируется один звуковой сигнал длительностью 1 с. В положении «ПОСТОЯННО» звуковой сигнал звучит постоянно до сброса блока кнопкой SA1.

Помимо работы устройства в режиме, когда излучатель направлен на приемник, можно направить их в одну сторону (конечно, исключив непосредственное попадание луча передатчика в приемник).

Таким образом, будет реализована схема **ИК-локатора** (например, для парковочного датчика автомобиля). Если же снабдить ИК передатчик и приемник собирающими линзами и направить их, например, на оконное стекло, то отраженный ИК сигнал будет промодулирован с частотой звуков в помещении.

Для прослушивания такого сигнала на выход DA2 необходимо подключить амплитудный детектор с усилителем низкой частоты и заменить C10, C11 конденсаторами емкостью 100 пФ, резисторы R21, R22— 300 кОм, R19, R20 — 3 кОм.

Вообще, от емкости конденсаторов C10, C11 интегратора зависит возможность получения большого уровня усиления. Чем емкость кон-

денсаторов больше, тем больше сглаживаются случайные помехи и тем больше можно получить усиление. Однако ради этого приходится жертвовать быстродействием устройства.

Противодействие снятию со стекла информации по ИК-каналу: строим модулятор стекла с плавающей частотой

Каждому действию всегда находится противодействие. Так для защиты информации были придуманы модуляторы стекла, т. е. устройства, создающие помехи, широкополосный акустический шум, модулирующий оконное стекло с псевдослучайной последовательностью.

Рассмотрим **модулятор стекла с плавающей частотой**, созданный на микросхеме К561ЛЕ5. Этот модулятор **предназначен** для создания помех устройствам, считывающим звуки с поверхности оконного стекла. Модулятор питается от сети переменного тока напряжением 220 В. Принципиальная схема модулятора приведена на **рис. 9.8**.

Напряжение сети гасится резисторами R1 и R2 и выпрямляется диодом VD1 типа КД102А. Конденсатор С1 уменьшает пульсации выпрямленного напряжения. Модулятор выполнен на одной микросхеме К561ЛЕ5. По своему схемному построению он напоминает генератор качающей частоты или частотный модулятор.

На элементах DD1.3 и DD1.4 собран управляющий генератор низкой частоты. С его выхода прямоугольные импульсы поступают на интегрирующую цепочку R5, С4.

При этом конденсатор С4 то заряжается через резистор R5, то разряжается через него. Поэтому на конденсаторе С4 получается напряжение треугольной формы, которое используется для управления генератором на элементах DD1.1, DD1.2.

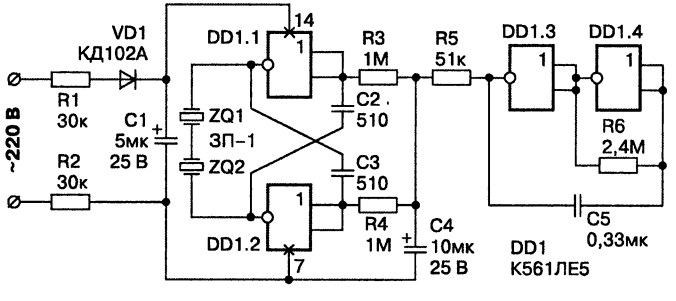


Рис. 9.8. *Схема модулятора стекла*

Этот генератор собран по схеме симметричного мультивибратора. Конденсаторы C2 и C3 поочередно заряжаются через резисторы R3 и R4 от источника треугольного напряжения. Поэтому на выходе генератора будет иметь место сигнал, частота которого «плавает» в области звуковых частот речевого диапазона. Поскольку питание генератора нестабилизировано, то это приводит к усложнению характера генерируемых сигналов. Нагрузкой генератора служат пьезокерамические излучатели ZQ1 и ZQ2 типа ЗП-1.

Микросхему DD1 можно заменить как на К561ЛА7, так и на К561ЛН1, К561ЛН2, либо на микросхемы серий 564, 1561.

Излучатели ZQ1 и ZQ2 могут быть любыми, их количество может быть от одного до четырех. Они приклеиваются к стеклу и могут быть соединены последовательно или параллельно-последовательно.

Противодействие снятию со стекла информации по ИК-каналу: строим модулятор стекла на трех КМОП микросхемах

Следующее устройство представляет собой **модулятор стекла,** построенный на трех КМОП микросхемах. Схема (**рис. 9.9**) включает в себя: задающий генератор на частоту 50 кГц (D1.1, D1.2); формирователь псевдослучайной последовательности импульсов на сдвигающих регистрах (D2, D3); логическую схему (D1.3, D1.4).

Звуковыми излучателями (HF1, HF2) являются телефонные капсюли ВП-1 или ДЭМ-4М. Резистор R4 позволяет регулировать громкость звука. Схема может питаться от любого нестабилизированного источника с напряжением от 4 до 15 В и потребляет ток не более 20 мА.

В качестве источника звука подойдут и любые малогабаритные динамики (с 50-омным сопротивлением), но при этом возрастет потребляемый ток. Транзисторы можно заменить на КТ829А. При правильной сборке схема **настройки** не требует. Устройство выполняется в виде переносной коробки и размещается на подоконнике, вблизи от стекла.

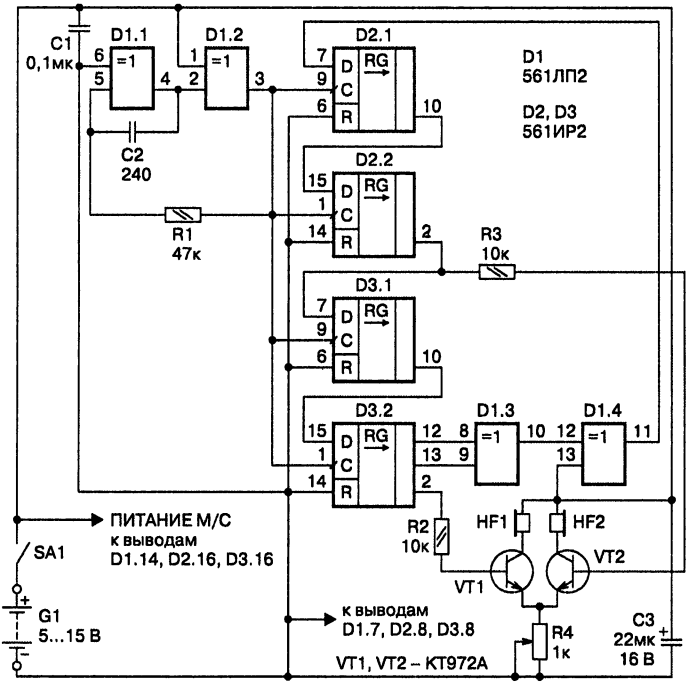


Рис. 9.9. Схема модулятора стекла на цифровых микросхемах

Противодействие снятию со стекла информации по ИК-каналу: строим модулятор оконного стекла на микросхемах К561ЛН2 и К561ИЕ8

Простой модулятор стекла вызывает вибрацию стекла с различной частотой, тем самым устраняя основной недостаток простейшего модулятора. Оно выполнено на двух цифровых схемах 561 серии. В качестве вибропреобразователя используется пьезокерамический преобразователь. Принципиальная схема устройства приведена на **рис. 9.10**.

Модулятор собран на микросхемах К561ЛН2 и К561ИЕ8. Генератор тактовых импульсов собран на элементах DD1.1, DD1.2, резисторе R1 и конденсаторе C1 по схеме несимметричного мультивибратора.

С выхода генератора тактовые импульсы поступают на вход счетчика DD2 типа К561ИЕ8. Эта микросхема имеет встроенный дешифратор. Поэтому напряжение высокого уровня поочередно появляется на выходах счетчика в соответствии с количеством пришедших импульсов.

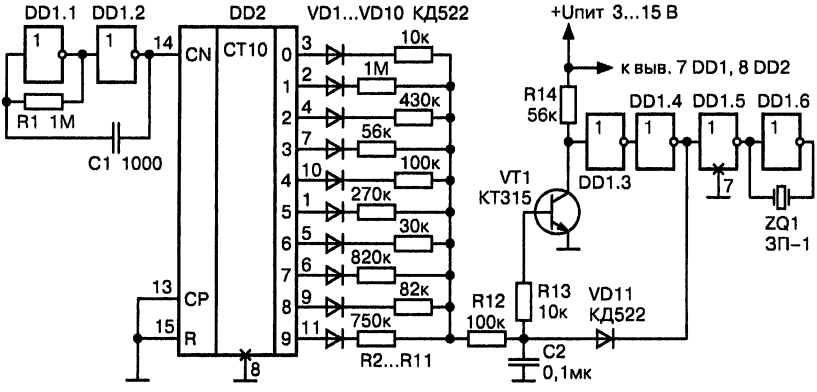


Рис. 9.10. *Схема модулятора стекла на двух цифровых схемах 561 серии*

Допустим, что после прихода очередного тактового импульса уровень логической единицы появился на выходе 2 микросхемы DD2 (выв. 4). На остальных выходах присутствует уровень логического нуля. Положительное напряжение начинает заряжать конденсатор C2 по цепи VD3, R4, R12.

При достижении на конденсаторе C2 напряжения, достаточного для открывания транзистора VT1 типа КТ-15, последний открывается, и на выходе элемента DD1.4 появляется уровень логического нуля. Конденсатор C2 быстро разряжается через диод VD11 типа КД522. Транзистор VT1 закрывается, и процесс заряда конденсатора C2 возобновляется по той же зарядной цепи.

С приходом очередного тактового импульса уровень положительного напряжения появляется только на выходе 3 (выв. 7). Теперь конденсатор C2 заряжается по цепи VD4, K5, R12. Так как суммарное сопротивление этой цепи меньше, чем сопротивление цепи VD3, R4, R12, то заряд конденсатора C2 до напряжения открывания происходит быстрее. Частота импульсов на выходе этого управляемого генератора увеличивается. Прямоугольные импульсы поступают на вибропреобразователь ZQ1, выполненный на основе пьезокерамического преобразователя.

Детали. Микросхемы DD1 и DD2 можно заменить на аналогичные — серий 176, 564, 1561. Резисторы — типа МЛТ-0,125. Сопротивления резисторов R2—R11 могут быть любыми из интервала 10—1000 кОм. Резисторы одинакового номинала лучше не использовать.

Диоды VD1—VD11 могут быть любыми, например, КД521, Д9, Д18, КД510 и др. Транзистор VT1 можно заменить на КТ3102. Пьезокерамический преобразователь ZQ1 может быть любой, от игрушек или телефонных аппаратов.

Питание устройства осуществляется от батарейки типа «Крона». Вибродатчик ZQ1 приклеивается на стекло клеем «Момент». Сигнал к нему подводится по проводам от элемента DD1.6.

Настройка заключается в установке частоты тактового генератора подбором конденсатора C1 или резистора R1. Частота тактовых импульсов выбирается около 2—3 Гц.

Противодействие снятию со стекла информации по ИК-каналу: строим генератор помех на микросхеме К561ИЕ10

Количество генерируемых частот можно увеличить, если вместо микросхемы DD2 К561ИЕ8 использовать широко распространенную микросхему К561ИЕ10. Эта микросхема (**рис. 9.11**) содержит два двоичных четырехразрядных счетчика.

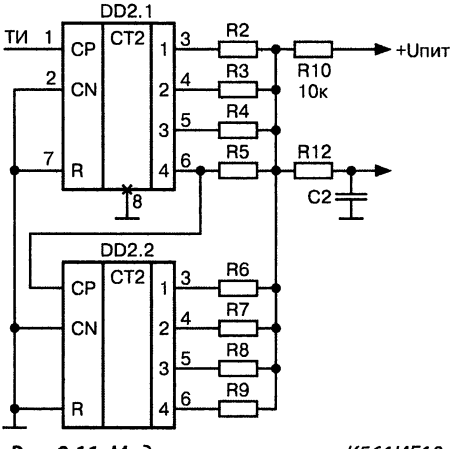


Рис. 9.11. Модулятор стекла на К561ИЕ10

К выходам счетчиков подключаются резисторы R2—R9, их сопротивления могут быть также от 10 кОм до 1 МОм. Диоды VD1—VD10 из схемы исключаются. При подаче тактовых импульсов на вход CP микросхемы DD2.1 в точке соединения резисторов R2—R12 появляется, изменяющееся ступенчато, напряжение.

Число градаций напряжения, а, следовательно, и число частот, можно варьировать путем использования определенного количества разрядов счетчика DD2.

СНЯТИЕ ИНФОРМАЦИИ С ТЕЛЕФОННОЙ ЛИНИИ И ПРОТИВОДЕЙСТВИЕ СНЯТИЮ

В настоящее время телефонные коммуникации все еще широко распространены. Вероятность использования телефонных линий для несанкционированного съема информации очень велика. В главе приведено большое количество схем для этого. Но помните, что использование этих устройств в некоторых случаях запрещено законодательством РФ и может привести к административной или уголовной ответственности.

Рассмотрены и устройства защиты телефонной линии, которые предназначены для регистрации факта подключения и самовольного коммерческого использования линии. Своевременная индикация позволяет абоненту предотвратить дальнейшие попытки подключения к его линии.

Телефонный адаптер с последовательным подключением

Схема (**рис. 10.1**) демонстрирует принцип записи звукового сигнала при последовательном подсоединении к телефонной линии. При протекании тока в линии постоянная и переменная составляющие телефонного сигнала создают падение напряжения на постоянном резисторе R1, включенном в разрыв одного из проводов линии.

Постоянная составляющая проходит через обмотку трансформатора T1 и один из встречно включенных светоизлучающих диодов оптронов DA1, DA2, вызывая отпирание транзистора VT1 и подачу положительного напряжения на выход управления. Звуковая составляющая сигнала через один из открытых светодиодов поступает на первичную обмотку звукового трансформатора T1 и создает звуковой сигнал во вторичной обмотке, нагруженной на резистор R6.

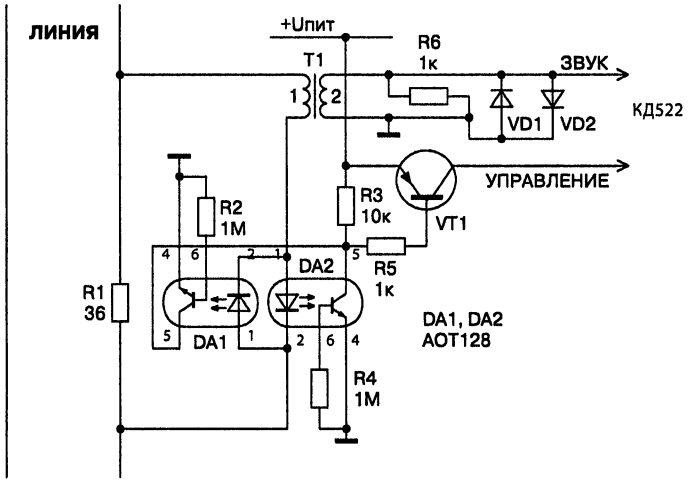


Рис. 10.1. Телефонный адаптер с последовательным подключением

Это интересно знать.
Последовательное включение в линию избавляет от необходимости настраивать устройство под различный уровень напряжения в линии.

Уровень звукового сигнала на выходе T1 достаточен для записи через микрофонный вход диктофона или ПК.

При желании один из оптронов можно убрать. Но тогда придется подбирать полярность подключения устройства к линии (или применить одну оптопару АОТ166 с двумя встречновключенными излучателями).

Это интересно знать.
Схема гальванически развязана от телефонной линии и безопасна для любого подключаемого устройства записи.

Оптроны, примененные в схеме, могут быть любыми транзисторными оптопарами со светоизлучающими диодами с рабочим током 5—10 мА, хорошо выдерживающими импульсные перегрузки. Сопротивление обмотки 1 звукового трансформатора T1 должно быть в пределах 20—40 Ом.

Коэффициент трансформации в пределах 1:1—3:1. Тип транзистора VT1 зависит от величины внешней нагрузки.

Радиоретранслятор с последовательным подключением к телефонной линии

Устройство, схема которого представлена ниже, представляет собой **УКВ ЧМ передатчик в радиовещательном диапазоне частот** (http://elektronicspy.narod.ru/TR.html). Питается оно от телефонной линии и имеет выходную мощность около 20 мВт.

Устройство подключается в разрыв одного из проводов линии в любом месте по всей длине кабеля. Принципиальная схема радиоретранслятора представлена на **рис. 10.2**.

Резистор R1 включается в разрыв одного из проводов телефонной сети. При снятии трубки телефонного аппарата в цепи появляется ток, который, в зависимости от типа аппарата и состояния линии, находится в пределах 10—35 мА. Этот ток, протекая через резистор R1, вызывает на нем падение напряжения порядка 4—25 В.

Напряжение поступает на выпрямительную диодную сборку типа КЦ407, благодаря которой устройство может подключаться в линию без соблюдения полярности. Высокочастотная часть схемы запитывается от параметрического стабилизатора, собранного на резисторе R3, стабилитроне VD3 типа КС191 и конденсаторе C7.

Стабилизатор ограничивает излишек напряжения, поступающего с диодной сборки VD1. Задающий генератор выполнен на транзисторе VT1 типа КТ315. Частотная модуляция осуществляется путем изменения емкости варикапа VD2 типа КВ109А. Модулирующее напряжение поступает из линии через последовательно включенные резистор R2 и конденсатор C1. Первый ограничивает уровень низкочастотного сигнала, второй — исключает проникновение постоянного напряжения линии в цепь модулятора.

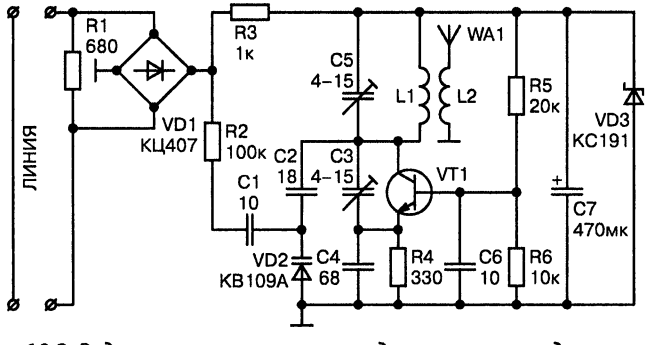


Рис. 10.2. Радиоретранслятор с последовательным подключением к телефонной линии

Частотно-модулированный сигнал с катушки связи L2 поступает в антенну, в качестве которой используется отрезок монтажного провода длиной, равной четверти длины волны, на которой работает передатчик.

Детали. Транзистор VT1 можно заменить на КТ3102, КТ368. Диодную сборку VD1 можно заменить на четыре диода КД102 или КД103. Стабилитрон VD3 можно использовать любой с напряжением стабилизации 6,8—10 В. Конденсатор С7 должен быть рассчитан на рабочее напряжение, большее напряжения стабилизации VD3.

Катушка L1 намотана на корпусе подстроечного конденсатора С5 и содержит 7 витков провода ПЭВ 0,31 мм. Катушка L2 намотана поверх катушки L1 тем же проводом — 2 витка. При **настройке** конденсаторы С3 и С5 подстраивают так, чтобы в нужном диапазоне (65—108 МГц) передавался сигнал максимально возможной мощности. Дальность действия собранного радиоретранслятора в зависимости от условий приема составляет 30—150 м.

Телефонный радиоретранслятор с амплитудной модуляцией в диапазоне частот 27—28 МГц

Телефонный радиоретранслятор с АМ в диапазоне частот 27—28 МГц рассмотрен на http://www.warning.dp.ua/tel22.htm.

Устройство представляет собой телефонный радиоретранслятор, позволяющий прослушивать телефонный разговор на радиоприемник диапазона 27—28 МГц с амплитудной модуляцией.

Устройство представляет собой маломощный однокаскадный передатчик с амплитудной модуляцией и кварцевой стабилизацией несущей частоты. Задающий генератор выполнен по традиционной схеме на транзисторе VT1 типа КТ315.

Режим транзистора по постоянному току задается резисторами R2 и R3. Кварцевый резонатор ZQ1 включен между коллектором и базой транзистора VT1. Он может быть любым, на одну из частот диапазона 27—28 МГц.

Контур, состоящий из катушки L2 и конденсатора С3, настроен на частоту кварцевого резонатора. С катушки связи L1 сигнал поступает в антенну, в качестве которой используются телефонные провода.

Дроссель Др1 служит для разделения высокочастотного и низкочастотного сигналов. Диод VD1 предохраняет устройство от выхода

из строя в случае неправильного подключения. Передатчик подключается параллельно телефонной трубке.

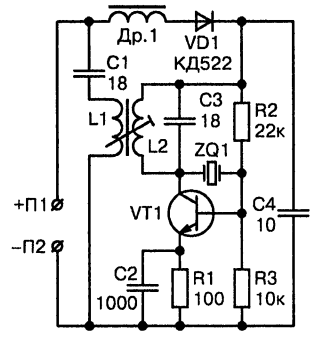


Рис. 10.3. Телефонный радиоретранслятор с АМ в диапазоне частот 27—28 МГц

Работа устройства. Когда трубка положена на рычаг, разговорный узел отключен от линии. Подключена к линии в этот момент только цепь вызывного устройства. Таким образом, до тех пор, пока трубка не снята, напряжение питания на передатчик не поступает.

Как только трубку снимают, к линии подключается разговорная часть. Во время разговора ток через разговорную часть меняется синхронно с речью, соответственно изменяется и напряжение в точках +Л1 и –Л1.

Изменение напряжения питания приводит к соответствующему изменению амплитуды генерируемых высокочастотных колебаний, т. е. имеет место амплитудная модуляция. В результате разговор можно слушать на расстоянии до 50 м на приемник диапазона 27—28 МГц, работающий на прием АМ сигнала.

Детали. Транзистор VT1 может быть типа КТ316, КТ3102, КТ368. Диод VD1 — КД521, КД510, Д220. Дроссель Др1 намотан на ферритовом стержне марки 600НН диаметром 2,8 мм и длиной 14 мм, он содержит 150—200 витков провода ПЭВ 0,1 мм.

Катушки L1 и L2 намотаны на полистироловом каркасе от КВ приемников диаметром 8 мм с подстроенным сердечником. Катушка L2 содержит 12 витков провода ПЭВ 0,31. Катушка связи L1 наматывается поверх катушки L2 и содержит 3 витка того же провода.

Настройка устройства осуществляется путем настройки контура L2, C3 на несущую частоту. При подключении следует учитывать полярность напряжения линии.

Телефонный УКВ ЧМ-ретранслятор на МОП-транзисторе

УКВ ЧМ ретранслятор рассмотрен на http://www.electroscheme.ru/sxems/8.html.

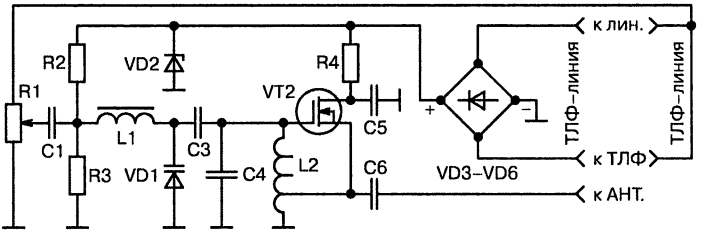


Рис. 10.4. УКВ ЧМ ретранслятор

На **рис. 10.4** представлен пример схемы телефонного УКВ ЧМ-ретранслятора на МОП-транзисторе. Схема собрана без УНЧ. Резистор R1 — регулятор громкости. При чувствительности УКВ-радиоприемника 10 мкВ дальность — около 100 м. Подключение данных УКВ ЧМ-ретрансляторов производится в соответствии со схемой. Передающей антенной служит отдельный провод.

Телефонный ЧМ передатчик на биполярном транзисторе

Телефонный ЧМ передатчик рассмотрен на http://ciscom.ru/hackersrussia/Spy/Telrets/tr9.php. Схема этого передатчика показана на **рис. 10.5.**

Предлагается усовершенствованная схема телефонного радиопередатчика с использованием телефонной линии в качестве антенны и имеющего стабилизатор напряжения. Это позволяет почти полностью устранить сетевой фон. Устройство можно закамуфлировать под телефонную розетку, конденсатор, распаечную коробку.

Катушку L1 наматывают на оправке диаметром 6 мм проводом ПЭВ 0,5 мм. Она содержит около 6 витков. Катушка L2 расположена поверх нее и имеет 3 витка того же провода.

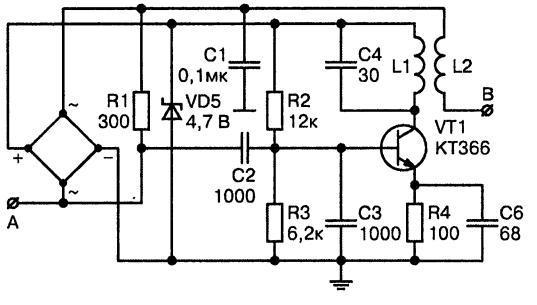


Рис. 10.5. Телефонный ЧМ передатчик

Возможно изготовление катушек прямо на плате печатным способом. При этом используется двухсторонний стеклотекстолит, а катушки для обеспечения связи располагают одна над другой. Передатчик включается в разрыв телефонной линии.

Телефонный жучок с питанием от телефонной линии

Телефонный жучок с питанием от телефонной линии рассмотрен на http://roma.3dn.ru/news/2007-02-16-163. Схема жучка показана на **рис. 10.6.**

Детали. L1 и L2 намотаны на оправках диаметром 5 мм, обмоточным проводом марки ПЭВ-1 или ПЭВ-2 диаметром от 0,4 до 0,7. L1 содержит 6 витков. L2 содержит 7 витков. Все катушки намотаны виток к витку и после настройки залиты парафином.

T1—T3 должны быть высоковольтные, такие как 2SC1279, 1515, 1570. Кварц работает на третьей гармонике. Подбираем так: выбираем частоту, делим на 3 и получаем частоту резонатора! Идем в магазин и покупаем. D5 любой стабилитрон с напряжением стабилизации 5—6 В. C10 — любой электролит емкостью от 10 до 100 мкФ и напряжением 6—10 В.

Это интересно знать.
Данное устройство подключается параллельно телефонной линии.

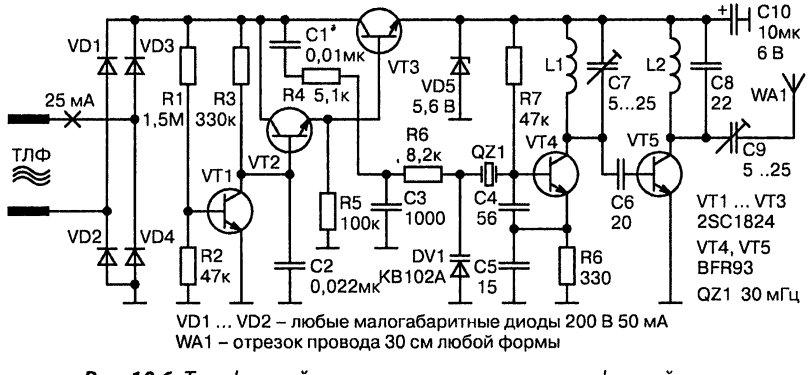


Рис. 10.6. *Телефонный жучок с питанием от телефонной линии*

Настройка. Налаживание устройства происходит в 6 этапов. Подключаем устройство к телефонной линии и переходим к стадии 2. Измеряем напряжение на D5, оно должно быть 5—5,6 В. Если напряжение не соответствует, то проверяем монтаж и исправность элементной базы.

Включаем контрольный приемник и пытаемся поймать сигнал передатчика! (все измерения и настройка проводится строго со снятой трубкой телефонного аппарата). Сигнал пойман, в противном случае проверяем монтаж и исправность того барахла, что вы туда впаяли.

Медленно поворачивая C7, добиваемся в приемнике максимально качественного и громкого сигнала на частоте третьей гармоники кварца, т. е. 96 МГц. Если этого не происходит, то можно попробовать подобрать C4 и, в крайнем случае, C5.

Изменением геометрических размеров L2 (раздвижением или сжатием витков не металлическим предметом) до максимального уровня выходного сигнала. Пластиковой отверткой регулируете положение ротора конденсатора C9 по минимальному току потребления и максимальной дальности передачи.

Радиус действия устройства составляет около 200 м на этой частоте и с этим потреблением тока — это предел. Большое потребление тока вызовет снижение громкости в трубке телефонного аппарата, что в свою очередь приведет к рассекречиванию устройства. А нам этого не нужно! Общий ток потребления устройства составляет 25 мА.

Бесконтактный съем информации с телефонной линии

Бесконтактный индуктивный способ снятия звуковой информации с телефонной линии известен давно. Он основан на эффекте возникновения магнитного поля вокруг проводника, по которому течет ток.

Правило.
Вокруг каждого из проводов, предающих ток, возникает магнитное поле, а у проводов пары оно противоположное.

Чтобы уловить и преобразовать это поле в электрический сигнал, необходимо только один из проводов пары пропустить сквозь магнитный сердечник, на котором имеется обмотка.

Таким образом, пропущенный провод выступит в роли первичной обмотки из одного витка, вторичная обмотка может иметь 200—600 витков.

Данная конструкция представляет собой классический **токовый трансформатор**, напряжение во вторичной обмотке которого пропорционально току в первичной обмотке, то есть в линии.

Совет.

*Катушку **индуктивного съемника** удобно выполнить на размыкающемся броневом или кольцевом ферритовом сердечнике с максимально высокой магнитной проницаемостью и имеющим возможно большее число витков. Для исключения низкочастотных наводок (особенно от сети) индуктивный съемник должен быть заключен в металлический экран.*

Такой датчик можно подключать непосредственно на микрофонный вход высококачественных диктофонов, имеющих высокое усиление сигнала внешнего микрофона и снабженных акустопуском.

Усилитель низкой частоты с акустопуском

Для записывающих устройств попроще можно применить **предусилитель с акустопуском**, выполненный на одной цифровой КМОП микросхеме К564ЛН2 по схеме **рис. 10.7**.

На инверторах DD1.1—DD1.3 выполнен усилитель низкой частоты. Элементы VD1, C4 образуют пиковый детектор, за которым следует компаратор на элементах DD1.5, DD1.6, управляющий силовым ключом на транзисторах VT1, VT2.

Величину резистора R1 можно подобрать по наилучшему качеству звука. Конденсатор C2 на выходе УНЧ служит для подавления возможного самовозбуждения УНЧ на высоких частотах. Резистором R2

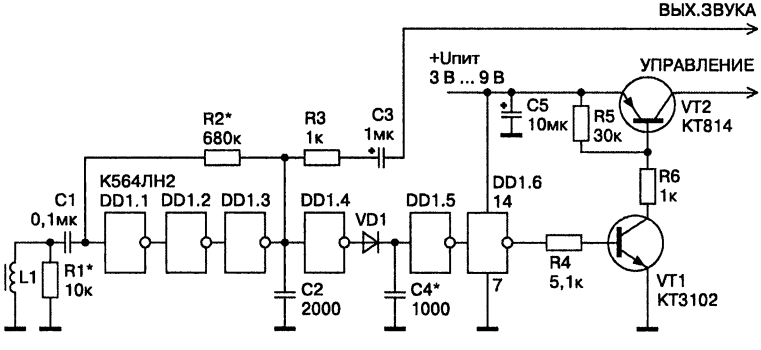


Рис. 10.7. Усилитель низкой частоты с акустопуском

можно подобрать требуемую величину усиления. От емкости и тока утечки конденсатора С4 зависит время удержания акустопуска.

Далее рассмотрим **устройства для бесконтактного съема информации с телефонной линии на ОУ.**

Устройства для бесконтактного съема информации с телефонной линии на ОУ

На **рис. 10.8, *а*** представлена **схема простого усилителя**, на вход которого подключена катушка индуктивности. В схеме можно применить ОУ — КР1407УД2, КР140УД20, КР1401УД2Б, КР140УД12, 140УД8 или аналогичные, в их типовом включении и желательно с внутренней коррекцией.

Это интересно знать.

Помещенная рядом с телефонным проводом катушка будет надежно «снимать» информацию.

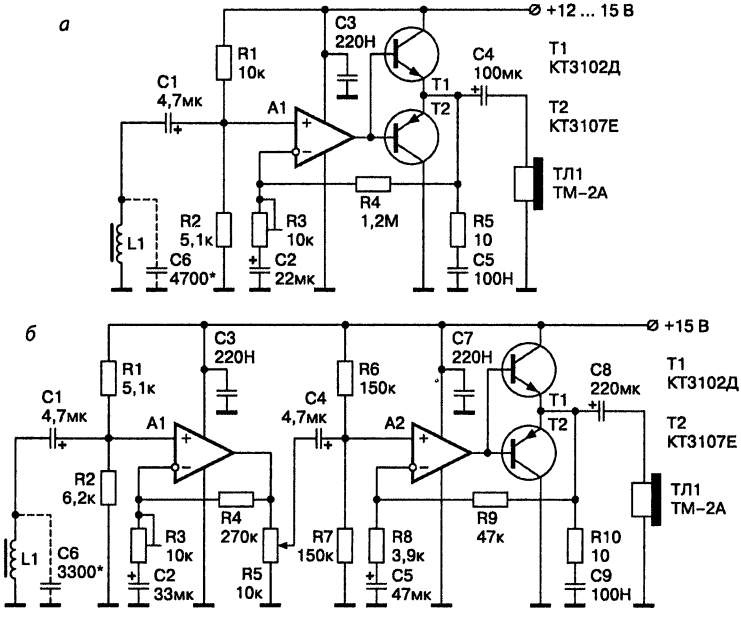


***Рис. 10.8.** Устройства для бесконтактного съема информации с телефонной линии на ОУ:*
а — простейшая схема; б — схема с возможностью регулирования громкости

Катушку-датчик можно выполнить на броневом сердечнике подходящего размера. Один из проводов телефонной пары зажимается между чашками броневого сердечника.

В качестве **катушки для бесконтактного съема информации** с телефонной линии можно использовать магнитную головку от кассетного магнитофона. В этом случае один из телефонных проводов просто располагается рядом с рабочим зазором головки.

Катушку-датчик так же можно изготовить и из малогабаритного низкочастотного трансформатора, например, выходного трансформатора от транзисторного приемника, последовательно соединив все его обмотки.

При использовании в качестве датчика магнитофонной головки L1 целесообразно использовать конденсатор C6 емкостью 3000—10000 пФ, который совместно с индуктивностью L1 образует колебательный контур, настроенный на частоту 1—1,5 кГц. Это позволяет увеличить уровень сигнала с датчика и увеличить соотношение сигнал/шум.

На **рис. 10.8, *б*** приведена схема усовершенствованного усилителя для бесконтактного съема информации с телефонной линии на двух ОУ и с возможностью регулировки громкости. Устройство разработано Александром Семьяном.

Устройство бесконтактного съема информации на микросхеме К548УН2

Бесконтактный съем информации с телефонной линии обеспечивает схема, представленная на **рис. 10.9**.

Принцип действия данного устройства заключается в улавливании переменного электромагнитного поля, наводимого вокруг телефон-

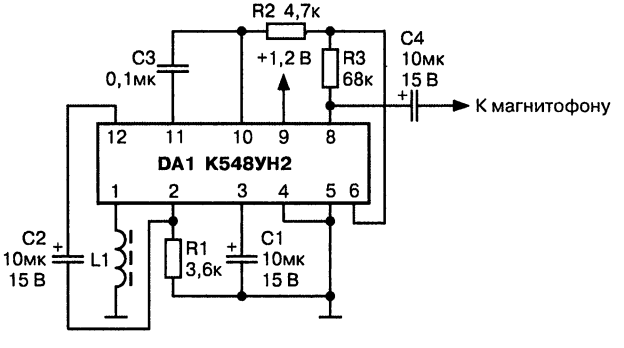


***Рис. 10.9.** Устройство бесконтактного съема информации*

ной пары (http://www.shematic.net/page-115.html). Для бесконтактного съема информации с телефонной линии телефонная пара зажимается между чашками броневого сердечника дросселя L1. Сигнал с усилителя попадает на микрофонный вход или на телефонный капсюль ТА-2. Напряжение питания должно быть в пределах 1,2—3 В. Дроссель L1 имеет 600 витков ПЭВ 0,05 на сердечнике СБ-30.

Назначение телефонных ретрансляторов

Телефонные ретрансляторы включаются последовательно в разрыв одного из проводов телефонной линии и питаются током в линии в момент разговора.

Это интересно знать.
Когда телефонная трубка опущена, ретранслятор не работает.

В широко распространенных схемах передатчик питается от падения напряжения на резисторе 200—500 Ом, частотная модуляция передатчика осуществляется изменением его напряжения питания.

Такое простое включение имеет, как минимум, два недостатка:

- девиация частоты передатчика сильно зависит от громкости разговора;
- частота самого передатчика может быть различной при различной нагрузке линии.

Например, при использовании старого дискового телефона и дешевого китайского разница частот передачи будет в несколько мегагерц.

Миниатюрный радиоретранслятор с частотной модуляцией

Это схема **миниатюрного ретранслятора с частотной модуляцией**, рассчитанного на работу в диапазоне УКВ на частотах 63—80 МГц совместно с любым бытовым радиоприемником (http://cxem.net). Схема питается от телефонной линии только во время разговора, когда поднята телефонная трубка. Прослушивается разговор радиоприемником на участке диапазона, где нет радиовещательных станций. Принципиальная схема радиоретранслятора представлена на **рис. 10.10, *а***.

Это интересно знать.

Радиус действия передатчика без применения антенны WA1 — до 50 м, а для увеличения дальности, кроме применения антенны, необходимо использовать приемник с высокой чувствительностью. Так, увеличение чувствительности приемника в 2 раза на столько же увеличивает дальность приема.

Настройка схемы заключается в перестройке генератора сердечником катушки L1 на нужную частоту УКВ диапазона, а после этого конденсатором C3 надо подстроить передатчик, контролируя прием по качеству передачи на слух.

Частотная модуляция в передатчике получается за счет изменения внутренней емкости транзистора при колебании напряжения питания схемы за счет протекания тока в линии ТА при разговоре.

Перед настройкой передатчика необходимо подключить его к телефонной линии и при снятой трубке замерить напряжение на резисторе R4. Оно должно быть в диапазоне от 2 до 3,5 В. Если напряжение больше, то следует уменьшить сопротивление этого резистора. Схема передатчика собрана на односторонней печатной плате размером 20×40 мм, к контактным площадкам которой припаиваются элементы.

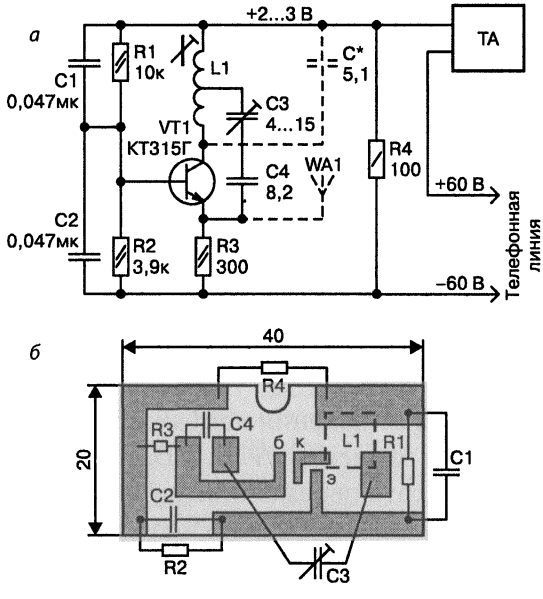


Рис. 10.10. *Миниатюрный радиоретранслятор с частотной модуляцией: а — принципиальная схема; б — печатная плата*

Размеры платы позволяют разместить ее в корпусе стандартного телефонного гнезда. **Печатная плата** представлена на **рис. 10.10, *б***.

Конденсатор С3 типа КПКМ, а остальные используемые резисторы и конденсаторы могут быть любого типа, малогабаритные. Катушка L1 наматывается на каркасе диаметром 5 мм проводом ПЭВ 0,23 мм и содержит 5+5 витков. Транзистор КТ315Г можно заменить на КТ3102А.

Совет.
Использовать другие транзисторы не рекомендуется, так как при этом сильно возрастает уровень гармоник, которые могут создавать помехи в других диапазонах.

В качестве антенны можно применить отрезок любого многожильного провода длиной 30—40 см. Настройку на нужную частоту, если нет высокочастотного ферритового сердечника, можно выполнить подбором емкости контура, показанного на схеме (**рис. 10.10, *а***) пунктиром. Конденсаторы С1 и С2 могут иметь номиналы 0,022—0,068 мкФ.

Это интересно знать.
Подключение данных схем никак не сказывается на качестве работы телефона. При подключении устройства к телефонной линии необходимо соблюдать полярность, указанную на схеме.

Телефонный радиоретранслятор на микросхеме КФ174ПС1

На одной микросхеме КФ174ПС1 можно собрать **телефонный ретранслятор**, в значительной степени не имеющий недостатков (**рис. 10.11**). Настройка его контуров осуществляется не подстроечными конденсаторами, а изменением расстояния между витками катушек.

Передатчик питается от падения напряжения на мощном стабилитроне, выполненном на элементах VT1, VD2, R2.

Благодаря этому частота передатчика не зависит от величины тока в линии. Вместо этих элементов можно использовать и обычный стабилитрон с постоянным допустимым током стабилизации не менее 50 мА. Звуковое напряжение для модуляции передатчика снимается с резистора R1.

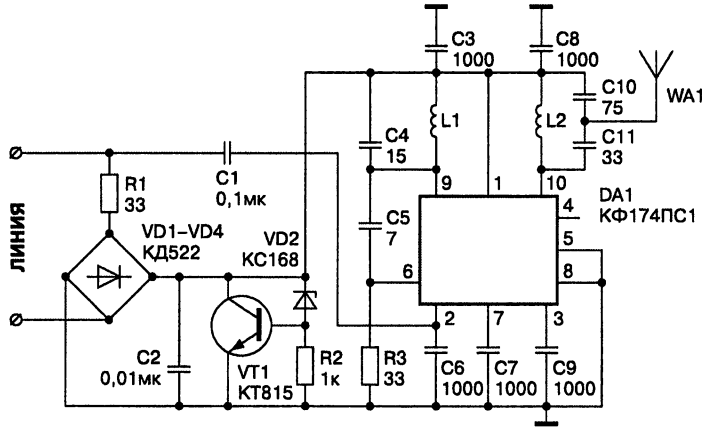


Рис. 10.11. Схема телефонного радиоретранслятора на ИМС КФ174ПС1

Антенна представляет собой кусок провода длиной четверть волны и включена в выходной контур через емкостный делитель С10, С11.

Телефонный ретранслятор с параллельным подключением к телефонной линии

Теперь рассмотрим **телефонный ретранслятор с параллельным подключением к линии.**

Это интересно знать.
Как правило, нагрузка в линии более 1 мА, при положенной телефонной трубке, нарушает работу телефонного аппарата.

Схема, приведенная на **рис. 10.12**, обходит эту проблему за счет использования узла автоматики, выполненного на транзисторах VT1, VT2.

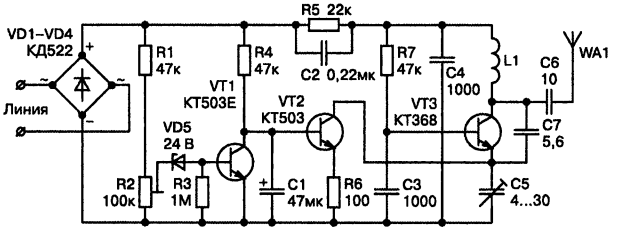


Рис. 10.12. Схема телефонного ретранслятора с параллельным подключением к линии

При положенной телефонной трубке устройство не активно и потребляет ток менее 0,5 мА (зависит от величин резисторов R1, R2 и стабилитрона VD5). При уменьшении напряжения в линии вследствие поднятия трубки, автоматика включает высокочастотный передатчик, выполненный на транзисторе VT3.

В этом случае устройство, даже потребляя заметный ток (более 3 мА), не нарушает работы линии. Ведь ток в линии при поднятой трубке имеет величину около 40 мА.

Чтобы не подбирать полярность подключения устройства, входное напряжение выпрямляется мостовым выпрямителем на диодах VD1—VD4. Через делитель R1, R2 и последовательно включенный стабилитрон VD5 постоянное напряжение линии поступает на транзисторный ключ VT1.

Подстроечным резистором R2 можно настраивать порог включения передатчика при различном напряжении линии.

При данном типе стабилитрона с напряжением стабилизации 24 В устройство можно настроить для работы с линией напряжением 40—60 В.

Это интересно знать.

Для расширения диапазона настроек (в сторону более низкого напряжения) можно взять стабилитрон с более низким напряжением стабилизации (например, на 9 В или 12 В).

Ключ VT2 непосредственно включает высокочастотный передатчик VT3. Цепочка R4, C1 формирует задержку более секунды на включения устройства для предотвращения включения передатчика при звонковом напряжении (переменное напряжение амплитудой 100—200 В 25 Гц).

Высокочастотный передатчик выполнен по схеме с общей базой и включается замыканием его эмиттера на землю через ключ VT2. Мощность передатчика зависит от величины резистора R5 (ограничение тока), а также от величины R7 (смещение).

Совет.

Величины этих резисторов не следует делать слишком малыми (с целью увеличения мощности), это может привести к уменьшению громкости звука в трубке.

Частотная модуляция передатчика происходит изменением его напряжения питания звуковым напряжением линии через конденсатор С2.

При достаточной громкости звука в линии или качественном приемнике этот конденсатор можно исключить.

Транзистор VT1 желательно взять достаточно высоковольтным (с напряжением Uкэ не менее 60 В), VT3 — высокочастотный с рабочей частотой не менее 300 МГц, VT2 — любой n-p-n.

Бескаркасная катушка L1 содержит 3 витка медного провода диаметром 0,7 мм и наматывается на оправке диаметром 12 мм.

Телефонный ретранслятор с ЧМ на одном транзисторе и с использованием линии в качестве антенны

Рассмотрим далее схему **телефонного ретранслятора с ЧМ на одном транзисторе** и возможностью использования телефонной линии в качестве антенны.

Этот ретранслятор работает в диапазоне 65—108 МГц и обеспечивает дальность передачи до 200 м (**рис. 10.13, *а***). В качестве антенны использован отрезок провода длиной 90 см.

Частота задающего генератора на транзисторе VT1 типа КТ315 определяется параметрами контура L1, С3. Дроссели Др1 и Др2 разделяют ВЧ и НЧ составляющие сигнала.

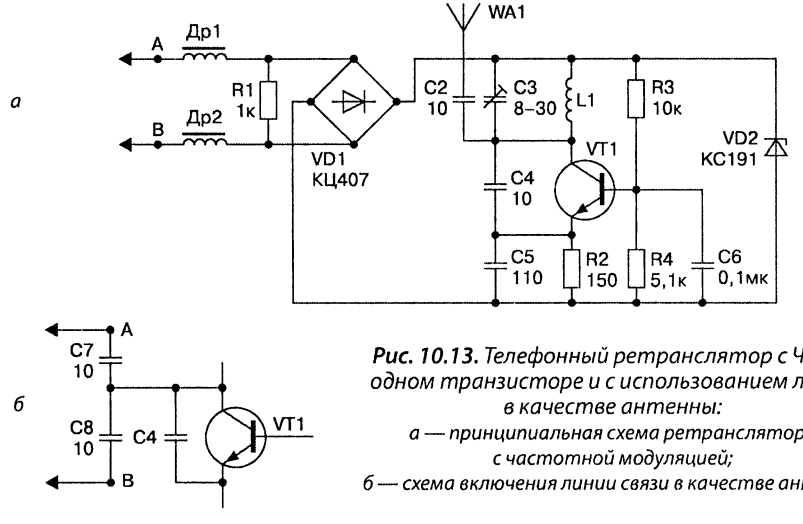


Рис. 10.13. *Телефонный ретранслятор с ЧМ на одном транзисторе и с использованием линии в качестве антенны:*
а — принципиальная схема ретранслятора с частотной модуляцией;
б — схема включения линии связи в качестве антенны

Это интересно знать.
В качестве антенны можно использовать и саму телефонную линию.

В этом случае конденсатор С2 нужно исключить, а устройство подключить к телефонной линии, как показано на **рис. 10.13, *б***.

Катушка L1 намотана на корпусе конденсатора С3 и содержит 4 витка провода ПЭВ 0,5 мм. Дроссели любые, индуктивностью 50—100 мкГн.

Телефонный ретранслятор на МОП-транзисторе с дополнительным усилителем

Телефонный УКВ ЧМ-ретранслятор с дополнительным усилителем может быть построен на МОП-транзисторе. На **рис. 10.14** представлена схема такого устройства. Для увеличения чувствительности в схему введен усилитель НЧ на транзисторе Т1. Резистор R1 — регулятор громкости.

При чувствительности УКВ радиоприемника 10 мкВ дальность действия ретранслятора — около 200 м. Подключение данных УКВ ЧМ-ретрансляторов производится в разрыв телефонной линии, она же используется в качестве антенны.

Катушка L2 — бескаркасная, имеет внутренний диаметр 6 мм, намотана проводом ПЭВ 0,8 мм, желательно посеребренным, содержит 3+1 витка. Дроссели L1—L3 применены готовые, индуктивностью 60—100 мкГн.

Настройка. Изменением величины резистора R2 следует установить напряжение на коллекторе транзистора Т1 равным половине напряжения питания. Увеличение сопротивления в коллекторе транзистора Т1 ведет к увеличению коэффициента усиления каскада.

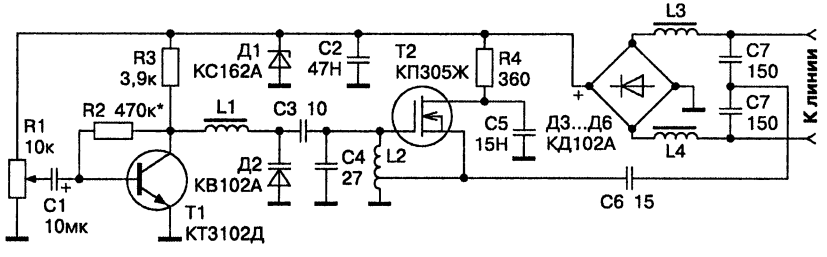


Рис. 10.14. Схема телефонного ретранслятора на МОП-транзисторе с дополнительным усилителем

Однако, не рекомендуется уменьшать коллекторный ток менее 0,5 мА, т. е. устанавливать R3 более 10—15 кОм.

При отсутствии генерации нужно подстроить (подобрать, начиная, например, с 500 Ом) резистор R4, не превышая допустимого предела максимального тока транзистора T2, равного 15 мА.

Совет.

Оптимальный ток стока должен составлять 12—14 мА. При этом токе обеспечивается максимальная мощность излучения, дальность передачи, стабильность частоты и минимальное влияние антенны.

При уменьшении тока стока МОП-транзистора повышается экономичность схемы, но ухудшаются перечисленные параметры.

Совет.

Не рекомендуется уменьшать ток стока менее 5 мА, иначе при подключении передающей антенны возможен не только значительный уход частоты, но даже срыв генерации.

Частота генерации устанавливается как конденсатором C4, так и сжатием или растягиванием катушки L2. Для этой схемы также не рекомендуется увеличивать емкость конденсатора C3.

Эта схема предоставлена радиолюбителем UA9VJH, за что ему большое спасибо.

Телефонный ЧМ-ретранслятор средней мощности

Теперь рассмотрим телефонный ЧМ-ретранслятор средней мощности, собранный на двух биполярных транзисторах.

Автогенератор этого радиоретранслятора собран по обычной двухтактной схеме (**рис. 10.15**) на транзисторах VT1 и VT2 типа КТ315.

Частотная модуляция происходит при изменении напряжения на базах транзисторов. **Частота радиопередатчика** определяется контуром L1, C5. Дроссель Др1 можно использовать любой, с индуктивностью 50—100 мкГн. Катушка L1 наматывается на корпусе конденсатора C5 и содержит 4 витка провода ПЭВ 0,5 мм с отводом от середины.

Катушка L2 намотана поверх L1 и имеет 2 витка того же провода. Стабилитрон VD2 — любой малогабаритный, с напряжением стабилизации 10—12 В.

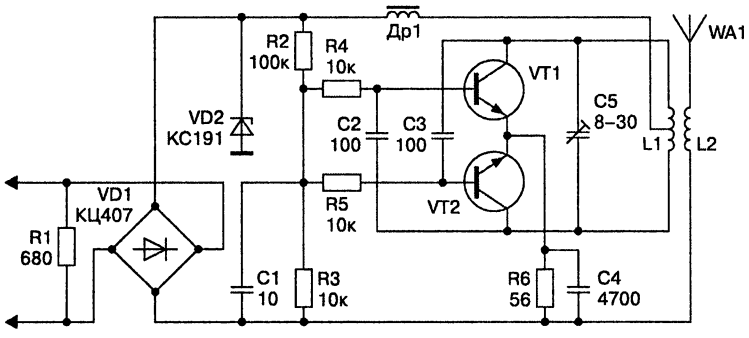


Рис. 10.15. *Схема телефонного ЧМ ретранслятора средней мощности*

Радиомикрофон-ретранслятор с питанием от телефонной линии

Рассмотрим универсальное устройство — **радиомикрофон-ретранслятор с питанием от телефонной линии.**

Это интересно знать.

Кроме вышеприведенных конструкций существуют комбинированные радиоретрансляторы, которые позволяют прослушивать не только сам телефонный разговор, но и разговоры в помещении, где этот радиоретранслятор установлен, причем при положенной трубке телефона.

Недостаток этих устройств — малая мощность, т. к. они питаются от телефонной линии и не могут потреблять ток более 1 мА. Схема такого устройства представлена на **рис. 10.16**.

Выпрямительный мост КЦ407 подключается параллельно телефонной линии. Напряжение в линии при положенной трубке составляет около 60 В. Это напряжение прикладывается к блоку питания, выполненному на элементах DA1, R1, VT1, VT2.

Микросхема DA1 типа КЖ101 представляет собой стабилизатор тока, работающий при напряжениях 1,8—120 В.

Падение напряжения при протекании стабильного тока через нагрузку во время заряда конденсатора C1 ограничено аналогом низковольтного стабилитрона на транзисторах VT1, VT2.

Это интересно знать.

При положенной трубке телефона устройство работает как радиомикрофон.

При поднятии трубки ТА незначительное изменение тока, протекающего через нагрузку — радиомикрофон, вызывает изменение рабочей точки транзистора VT3 и, тем самым, осуществляет частотную модуляцию радиомикрофона. Задающий генератор собран на транзисторе VT1 типа КТ368, режим работы по постоянному току задается резистором R1.

Частота колебаний задается контуром в базовой цепи транзистора VT1. Этот контур включает в себя катушку L1, конденсатор C3 и емкость цепи база-эмиттер транзистора VT1, в коллекторную цепь которого включен контур из катушки L2 и конденсаторов C6 и C7. Конденсатор C5 включен в цепь обратной связи и позволяет регулировать уровень возбуждения генератора.

Это интересно знать.

В автогенераторах подобного типа частотная модуляция производится путем изменения потенциалов выводов генерирующего элемента.

В схеме, приведенной на **рис. 10.16**, управляющее напряжение прикладывается к базе транзистора VT1, изменяя тем самым напряжение (емкость) на переходе база-эмиттер.

Изменение этой емкости приводит к изменению частоты генератора, чем и обеспечивается частотная модуляция. При использовании УКВ приемника зарубежного производства требуемая величина максимальной девиации несущей частоты составляет 75 кГц и получается при изменении напряжения звуковой частоты на базе транзистора в диапазоне 10—100 мВ.

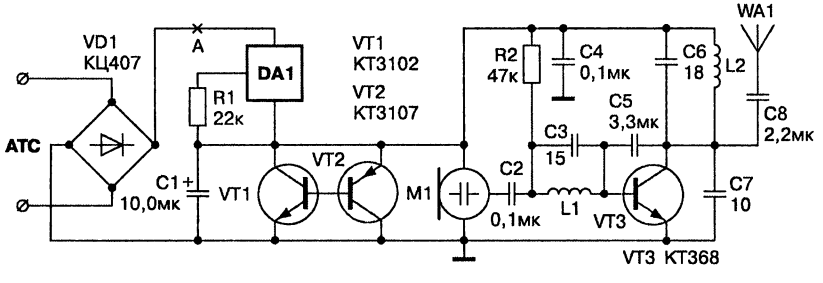


Рис. 10.16. Схема ретранслятора с питанием от телефонной линии

Это интересно знать.
Именно поэтому в данной конструкции не используется модулирующий усилитель звуковой частоты.

При использовании электретного микрофона со встроенным усилителем, уровня сигнала, снимаемого с его выхода, оказывается достаточно для получения требуемой девиации частоты передатчика.

Конденсатором С7 в небольших пределах можно изменять значение несущей частоты. Сигнал в антенну поступает через конденсатор С8.

Антенна изготовлена из куска медного провода длиной 60—100 см.

Катушки радиомикрофона бескаркасные, диаметром 2,5 мм, намотаны виток к витку:

- **катушка L1** имеет 8 витков провода ПЭВ 0,3 мм;
- **катушка L2** имеет 6 витков провода ПЭВ 0,3 мм.

При настройке устройства добиваются получения максимального сигнала высокой частоты, изменяя индуктивности катушек L1 и L2. Настройкой резистора R1 добиваются, чтобы ток в точке «А» был равен 1,5 мА.

Эту схему разработал Семьян А. П. в процессе экспериментов с различными схемами «жучков».

Устройство прослушивания способом высокочастотного навязывания

На **рис. 10.17** приведена схема прослушивания с использованием ВЧ-наводки относительно общего корпуса (в качестве которого лучше использовать землю, трубы отопления и т. д.) на один провод подайте ВЧ колебания 150 Гц выше. Через элементы схемы

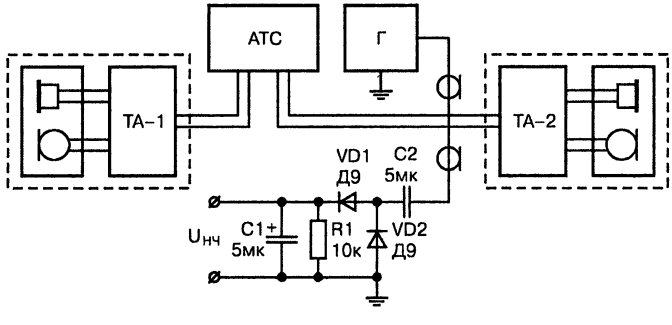


Рис. 10.17. Схема прослушивания способом высокочастотного навязывания

ТА, даже если трубка лежит на аппарате ВЧ колебание поступает на микрофон и далее уже промодулированное в линию. Этот метод называют «высокочастотным навязыванием», отмечается на http://spying.by.ru/spying/page_04_spying.shtml.

Промодулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления готов для прослушивания или записи. Дальность действия такой системы из-за затухания ВЧ-сигнала в двухпроводной линии не превышает нескольких десятков метров.

Суть этого способа состоит в следующем. На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА2, подаются колебания частотой 150 кГц и выше от генератора Г. В этом случае ВЧ-колебания проходят через микрофон или элементы схемы телефонного аппарата ТА2, обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения. К другому проводу линии подключается детектор, выполненный на элементах С1, С2, VD1, VD2 и R1. Детектор приемника выделяет речевую информацию, которая усиливается до необходимого уровня и обрабатывается. Корпус передатчика (генератор Г) и приемника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

Устройство для высокочастотного съема информации с телефонного аппарата

В завершении рассмотрим **устройство для высокочастотного съема** информации с телефонного аппарата.

Большинство вышеописанных устройств объединяет то обстоятельство, что получение информации идет во время телефонного разговора, т. е. телефон в это время работает.

А что происходит в перерывах, когда телефон не работает, а телефонная трубка находится на аппарате? Телефонная цепь разомкнута, а микрофон отключен. Опасаться вроде нечего.

Это интересно знать.

Реально не представляют большой сложности устройства, позволяющие использовать микрофон неактивного телефона для прослушивания помещения. Это становится возможным при использовании специальных методов и схем, предусматривающих применение ВЧ-колебаний.

Схема, реализующая этот способ, представлена на **рис. 10.18**. В основу ее работы положен принцип модуляции ВЧ-колебаний звуковым сигналом от микрофона телефонного аппарата (ТА).

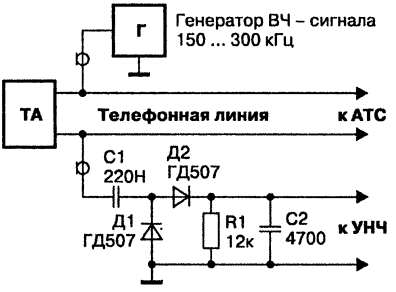


Рис. 10.18. Схема устройства для высокочастотного съема информации с телефонного аппарата

Для ВЧ-колебаний не является помехой разрыв цепей в ТА. Относительно общего провода, в качестве которого используют физическую «землю» (например, трубы отопления или «зануление» от электрического щита), на один из проводов телефонной линии от генератора подается ВЧ-колебания частотой 150 кГц и выше.

Даже если трубка лежит на аппарате, эти колебания поступают на микрофон телефонного аппарата:

- через элементы ТА;
- через индуктивные и емкостные связи между данными элементами, проводами, замкнутыми и разомкнутыми контактами.

Далее эти колебания, уже промодулированные звуковым сигналом с микрофона, — передаются обратно в линию. **Прием информации** производится относительно общего провода уже через второй провод телефонной линии.

После детектирования сигнал НЧ подается на УНЧ для усиления до необходимого уровня.

Эта схема использовалась для экспериментов с различными телефонными аппаратами при проверке систем защиты от прослушки.

Схемы для комплексной защиты телефонных аппаратов и линий связи

Эта схема (**рис. 10.19, *а***) включается между линией и телефонным аппаратом и практически полностью исключает прослушивание помещения, как методом усиления слабых сигналов, так и от высокочастотного навязывания.

Диоды VD1—VD4, включенные встречно-параллельно, защищают цепь звонка телефоного аппарата. Конденсаторы и катушки образуют фильтры С1, L1 и С2, L2 для подавления напряжений высокой частоты.

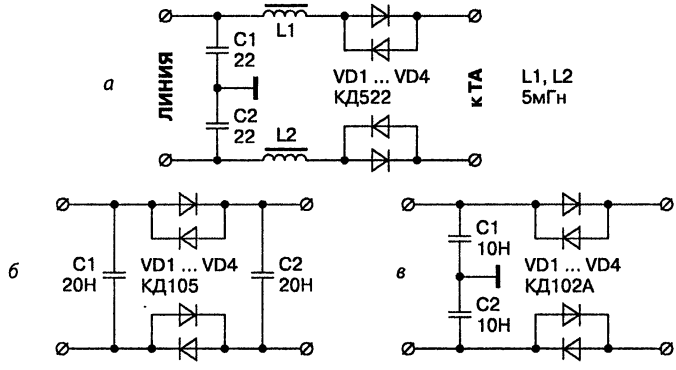


Рис. 10.19. *Схемы для комплексной защиты телефонных аппаратов и линий связи: а — первый вариант; б — второй вариант; в — третий вариант*

Детали монтируются в отдельном корпусе навесным монтажом. Устройство не нуждается в настройке. Однако оно не защищает пользователя от непосредственного подслушивания путем прямого подключения в линию.

Кроме рассмотренной схемы существует и ряд других, которые по своим характеристикам близки к ранее описанным устройствам. На **рис. 10.19, *б*, *в*** приведены **еще две схемы для комплексной защиты телефонных аппаратов и линий связи**, часто используемые в практической деятельности.

Индикатор состояния линии на микросхеме КР1407УД2

Сначала рассмотрим **индикатор состояния линии** на микросхеме КР1407УД2. Индикатор предназначен для оперативного контроля состояния телефонной линии. Он устанавливается в корпус телефонного аппарата и питается от телефонной линии. Контроль состояния (напряжения) линии происходит в момент ведения разговора, т. е. когда трубка снята и напряжение изменяется. Когда происходит постороннее подключение, то загорается светодиод.

Основу схемы (**рис. 10.20, *а***) составляет операционный усилитель на микросхеме DA1 типа КР1407УД2, включенный по схеме компаратора. При разговоре напряжение с линии подается через диод VD4 типа КД522 на параметрический стабилизатор напряжения на стабилитроне VD5.

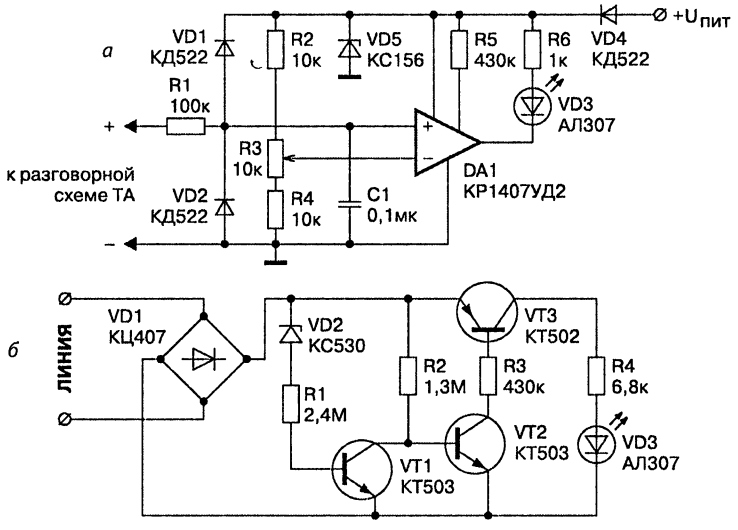


Рис. 10.20. *Индикаторы состояния линии:*
а — схема индикатора состояния линии на микросхеме КР1407УД2;
б — схема светового анализатора телефонной линии

Одновременно напряжение поступает на неинвентирующий вход ОУ. При снижении входного напряжения до уровня меньшего, чем опорное, на выходе компаратора появляется уровень логического нуля, и светодиод загорается. Резистором R5 устанавливается режим работы компаратора.

Сняв трубку телефонного аппарата и позвонив кому-либо, во время разговора постройкой резистора R3 добиваются погасания светодиода. Медленно изменяя сопротивление R3, находят момент срабатывания устройства, затем немного поворачивают движок резистора назад, светодиод гаснет. Прибор настроен.

В индикаторе вместо указанного ОУ можно применить КР140УД1208.

Будьте осторожны.
При подключении прибора следует соблюдать полярность!

Световой анализатор телефонной линии

Теперь рассмотрим **световой анализатор телефонной линии.** Данное устройство также является простейшим индикатором наличия подслушивающих устройств. Оно устанавливается на предвари-

тельно проверенной телефонной линии и контролирует линию при отсутствии разговора, когда трубка лежит на аппарате.

Питание анализатора (**рис. 10.20, *б***) осуществляется от телефонной линии. При наличии любых несанкционированных подключений различных устройств, питающихся от телефонной линии и вызвавших изменение напряжения в ней, выдается сигнал тревоги (включается красный светодиод).

Устройство (**рис. 10.20, *б***) включает в себя:

- анализатор, собранный на стабилитроне VD2 типа КС530 и транзисторе VT1 типа КТ503;
- усилитель тока, собранный на транзисторах VT2 и VT3 типа КТ503 и КТ502, соответственно.

К выходу усилителя через ограничительный резистор R4 подключен светодиод VD3 типа АЛ307. Выпрямительный мост VD1 типа КЦ407 обеспечивает требуемую полярность питания устройства независимо от полярности подключения его к телефонной сети.

При свободной линии постоянное напряжение в ней составляет около 60 В. Стабилитрон VD2 открывается, и на базу транзистора VT1 подается управляющий ток через резистор R1. Открытый транзистор VT1 шунтирует вход каскада на транзисторе VT2, поэтому усилитель тока закрыт, а светодиод погашен. При подключении в линию посторонних устройств напряжение в ней падает, и процесс переключения транзисторов происходит в обратном порядке, светодиод загорается.

Устройство защиты от несанкционированного подключения к телефонной линии

Устройство защиты от несанкционированного подключения к телефонной линии предназначено для кодирования линии индивидуальным одно-, двух-, трехзначным кодом. Оно применяется в тех случаях, когда имеется возможность установить устройство защиты в щитке, колодце, т. е. как можно дальше от охраняемого телефонного аппарата (в идеальном случае — на выходных клеммах АТС).

Система охраняет линию «за собой». При этом все посылки вызова, пришедшие с АТС, беспрепятственно допускаются к телефону, но для подключения к линии (ведения разговора, набора номера) на диске телефона (клавиатуре) необходимо набрать индивидуальный код.

Схема системы приведена на **рис. 10.21.** Устройство собрано на дискретных общедоступных элементах и микросхеме серии 561 с микропо-

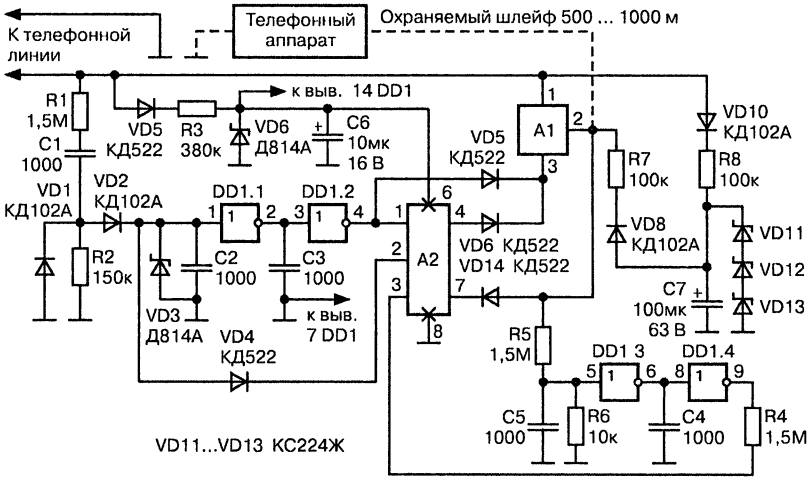


Рис. 10.21. *Устройство защиты от несанкционированного подключения*

треблением в статическом режиме. Вся схема питается от телефонной линии. В режиме ожидания потребление не превышает 10—20 мкА, в режиме приема вызова или обработки кода — 150—200 мкА.

В состав устройства входят:

- узел обработки импульсов вызова на элементах DD1.1, DD1.2;
- узел приема кода на элементах DD1.3, DD1.4;
- ключ включения телефона A1;
- дешифратор кода A2;
- узел питания на элементах VD7, R3, C6, VD8;
- узел питания напряжением 60 В на элементах VD10, R8, VD9, C7, R7, VD11—VD13.

Рассмотрим работу системы защиты.

Исходящая связь. При снятии трубки с телефона, подключенного в любом месте охраняемой части линии, в телефоне будет отсутствовать сигнал готовности станции (425 Гц). После набора соответствующего кода на диске (клавиатуре) телефона и обработки его узлом приема кода DD1.3, DD1.4 на выходе 4 дешифратора A2 появится уровень логической единицы, который через ключ A1 подключит телефон к линии (если код набран правильно).

Если код набран неправильно, система защиты блокируется на время 15—30 с, после чего можно повторить набор кода. При включении ключа A1 телефон работает в обычном режиме, обеспечивая

набор номера и связь. Система вновь входит в режим охраны через 10—20 с после того, как трубка будет опущена на аппарат.

Входящая связь. Любая посылка вызова частотой 25 Гц и напряжением 90—120 В, пришедшая от АТС, напрямую на телефон не поступает, так как ключ А1 в исходном состоянии заперт. После обработки сигнала вызова элементами DD1.1, DD1.2 с небольшой задержкой, определяемой номиналами элементов С2, С3, на выходе 4 DD1.2 появится логическая единица, которая через диод VD5 открывает ключ А1 только на время вызова. При снятии трубки с телефонного аппарата входной узел запирается через диод VD4, и далее для подключения телефона к линии и ведения разговора необходимо вновь набрать индивидуальный код.

Таким образом, система защиты блокирует подключение к охраняемому участку линии любых телефонных аппаратов без знания кода. Дешифратор может быть выполнен одно-, двух-, трехзначным.

Размер платы — 100×60 мм, подключение к линии осуществляется тремя разъемами. Единственным условием является использование телефонных аппаратов II и III группы сложности (с потреблением от линии не более 50—80 мкА).

Активный индикатор состояния линии

Активный индикатор состояния линии, в отличие от выше приведенного устройства, не только выявляет подключение дополнительной нагрузки, но и при срабатывании системы сигнализации переводит устройство в активный режим работы. Этот режим позволяет блокировать многие радиоретрансляционные устройства и приборы, предназначенные для автоматической записи телефонных переговоров. Принципиальная схема такого устройства представлена на **рис. 10.22.**

Устройство собрано на 4 микросхемах и 4 транзисторах. **Исходное состояние**: трубка телефонного аппарата опущена. Питание устройства осуществляется от телефонной линии через ограничительный резистор R5. Конденсатор С2 заряжается через резистор R5 до напряжения стабилизации стабилитрона, выполненного на транзисторе VT2.

С конденсатора С2 напряжение величиной 7—8 В поступает на устройство для питания микросхем (точка ***а***). От источника питания

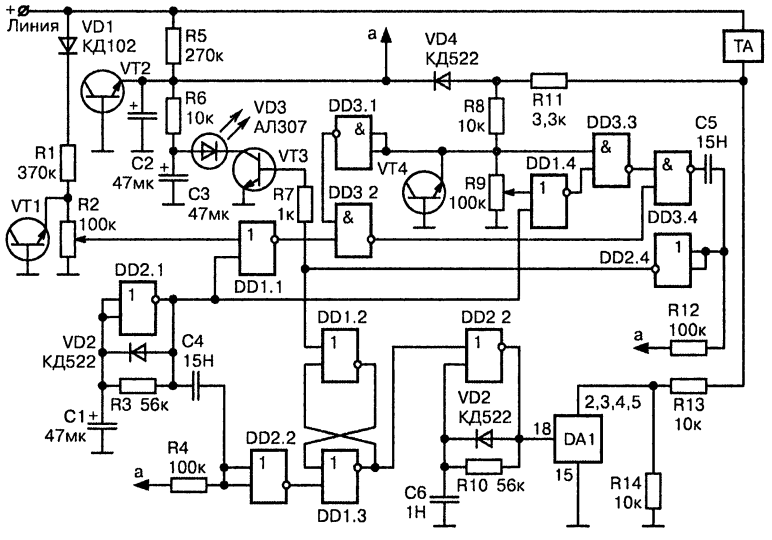


Рис. 10.22. Активный индикатор состояния линии

через резистор R6 заряжается конденсатор C3. Резисторы R6, R7, конденсатор C3, светодиод VD3 и транзистор VT3 образуют схему индикации устройства.

Напряжение линии через диод VD1 типа КД102 поступает на делитель напряжения, образованный резисторами R1 и R2. Напряжение на резисторе R2 ограничивается транзистором VT1, включенным по схеме стабилитрона до напряжения питания, что необходимо для защиты входов микросхем от высокого напряжения.

С движка подстроечного резистора R2 напряжение высокого уровня поступает на вход элемента DD1.1 микросхемы К561ЛЕ5, запрещая проход импульсов с генератора, выполненного на элементе DD2.1 микросхемы К561ТЛ1. Этот генератор собран на основе триггера Шмидта. При заряде и разряде конденсатора C1 на выходе генератора появляются прямоугольные импульсы.

Поскольку заряд конденсатора C1 происходит через диод VD2 типа КД522, а разряд — через резистор R3, то на выходе элемента DD2.1 имеют место короткие положительные импульсы с частотой следования 1—0,5 Гц. Первый же импульс, пройдя через дифференцирующую цепочку C4, R4 и элемент DD2.2, устанавливает триггер, собранный на элементах DD2.1, DD1.3, в положение, когда на входе элемента DD2.3 низкий уровень напряжения. Генератор, собранный на DD2.3, выключен и на выводах 1, 8 микросхемы DA1 типа КР1014КТ1 присутствует

высокий уровень. Одновременно импульсы с DD2.1 поступают на элементы DD1.1 и DD1.4. Через DD1.1 импульсы не проходят, так как с резистора R2 поступает высокий уровень. Нулевой уровень, снимаемый с резистора R9, подается на входы элементов DD3.1 и вход DD3.3 микросхемы К561ЛА7. Поэтому импульсы, проходящие через DD1.4, не проходят на DD3.4. Следовательно, на выходе DD2.4 присутствует логический нуль, и транзистор VT3 закрыт. С движка резистора R2 снимается напряжение логической единицы, достаточное для переключения элемента DD1.1, выполняющего функцию управляемого компаратора с чувствительностью в десятки милливольт.

Это интересно знать.

Если к линии подключается дополнительная нагрузка сопротивлением менее 100 кОм, то напряжение в линии уменьшится на некоторую величину.

Одновременно уменьшается и напряжение на движке резистора R2. Это приводит к появлению на входе DD1.1 напряжения, воспринимаемого микросхемой как уровень логического нуля. Этот уровень разрешает прохождение импульсов от DD2.1 через DD1.1. Поскольку на выходе DD3.1 высокой уровень, то импульсы проходят через ключ DD3.2. При этом на выходе DD3.3 тоже высокий уровень и эти импульсы проходят и через ключ DD3.4.

Продифференцированные импульсы цепочкой C6, R12 и элементом DD2.4 поступают на базу транзистора VT3. Транзистор открывается, и конденсатор C3 быстро разряжается через открытый транзистор VT3 и светодиод VD3, который ярко вспыхивает с частотой 0,5—1 Гц. В перерывах между импульсами конденсатор C3 подзаряжается через резистор R6. Так как оценка состояния линии происходит под управлением импульсов с генератора DD2.1, то некоторое изменение напряжения в линии в момент заряда конденсатора C3 на работе устройства не сказывается.

Рассмотрим случай, когда телефонная трубка снята. При этом сопротивление телефонного аппарата включается между плюсовым проводом линии и резисторами R11 и R13. Напряжение в линии уменьшается до 5—25 В, так как нагрузкой линии будут телефонный аппарат, резистор R13 и резистор R14, зашунтированный малым (около 10 Ом) сопротивлением микросхемы DA1.

Напряжение, снимаемое с резистора R13, обеспечивает питание устройства через диод VD4 типа КД522. При этом напряжение высокого уровня с точки соединения резисторов R8, R9 поступает на элементы DD3.3 и DD3.1. Низким уровнем закрывается ключ DD3.2. С движка резистора R9 снимается напряжение логической единицы, близкое к напряжению переключения компаратора DD1.4. Допустим, что к линии подключается (или была подключена) дополнительная параллельная или последовательная нагрузка, которая приводит к уменьшению напряжения в линии.

При этом напряжение на движке резистора R9 принимает уровень, расцениваемый микросхемой как уровень логического нуля. При этом импульсы с DD2.1 проходят через DD1.4, DD3.3 и DD3.4. После дифференцирующей цепочки C6, R12 и элемента DD2.4 они поступают на базу транзистора VT3, включая световую индикацию. Одновременно первый же импульс переводит триггер на DD1.2 и DD1.3 в состояние, разрешающее работу генератора на элементе DD2.3. С выхода генератора короткие импульсы частотой 12—20 кГц поступают на ключ, выполненный на микросхеме DA1.

Ключ начинает закрываться и открываться с частотой генератора. При этом сигнал в линии модулируется данной частотой, это вызывает расширение спектра сигнала, излучаемого радиоретранслятором, подключенным в линию.

Одновременно напряжение в линии увеличивается до 35—45 В. Это связано с тем, что последовательно с резистором R13 включается резистор R14, ранее шунтированный ключом DA1. Повышение напряжения в линии до такого уровня позволяет нейтрализовать автоматические записывающие устройства, срабатывающие по уровню напряжения в линии.

Для того чтобы работа этого генератора не мешала анализу состояния линии, он периодически отключается путем переключения триггера DD1.2, DD1.3 на момент оценки состояния линии. Если в процессе оценки состояния линии принимается решение о том, что линия свободна от посторонних подключений, то схема автоматически устанавливается в исходное состояние и переходит в ждущий режим с периодической проверкой состояния линии.

Детали. Резисторы используются типа МЛТ-0,125. Диод VD1 можно заменить на КД105, Д226. Транзисторы можно заменить на КТ3102,

КТ503. Микросхемы можно использовать из серий 564 и 1561. Конденсаторы С1, С2 и С3 должны быть с минимальным током утечки.

Настройка. При настройке устройства устанавливается частота генераторов 0,5—1 Гц и 12—20 кГц резисторами R3 и R10, соответственно. При включенном генераторе DD2.3 резистором R14 устанавливается уровень напряжения в линии, равный 35—45 В, при котором еще не происходит рассоединения линии. Исходные уровни срабатывания рассматриваемого устройства устанавливаются резисторами R2 и R9.

Будьте осторожны.
Прибор необходимо подключать к линии с соблюдением полярности!

Скремблеры

Кардинальной мерой предотвращения прослушивания телефонных разговоров является использование криптографических методов защиты информации, отмечается на http://www.spystuff.pdf. В настоящее время для защиты телефонных сообщений применяют два метода: преобразование аналоговых параметров речи и цифровое шифрование. Устройства, использующие эти методы, называются **скремблерами**.

При аналоговом скремблировании производится изменение характеристики исходного звукового сигнала таким образом, что результирующий сигнал становится неразборчивым, но занимает ту же частотную полосу. Это дает возможность без проблем передавать его по обычным телефонным каналам связи.

При этом методе сигнал может подвергаться следующим преобразованиям: частотная инверсия; частотная перестановка; временная перестановка.

При цифровом способе закрытия передаваемого сообщения непрерывный аналоговый сигнал предварительно преобразуется в цифровой вид. После чего шифрование сигнала происходит обычно с помощью сложной аппаратуры, зачастую с применением компьютеров.

Ниже приводится описание скремблера, использующего метод частотной инверсии. Этот метод давно и успешно применяется американскими полицейскими службами и обеспечивает эффективную

защиту радио- и телефонных переговоров от постороннего прослушивания.

Частотно-инвертированный сигнал выделяется из нижней боковой полосы спектра балансного преобразования звукового сигнала с надзвуковой несущей. Две последовательные инверсии восстанавливают исходный сигнал. Устройство работает как кодер и декодер одновременно.

Синхронизации двух скремблеров не требуется. Принципиальная схема такого скремблера приведена на **рис. 10.23**.

Это устройство состоит из таких элементов:

- тактового генератора на микросхеме DD2 типа К561ЛА7, вырабатывающего сигнал частотой 7 кГц;
- делителя-формирователя несущей 3,5 кГц на микросхеме DD3.1 типа К561ТМ2;
- аналогового коммутатора;
- балансного модулятора на микросхеме DD4 типа К561КТ3;
- входного полосового фильтра с полосой пропускания 300—3000 Гц на микросхеме DA1.1 типа К574УД2;
- сумматора балансного модулятора с фильтром низкой частоты на микросхеме DA1.2.

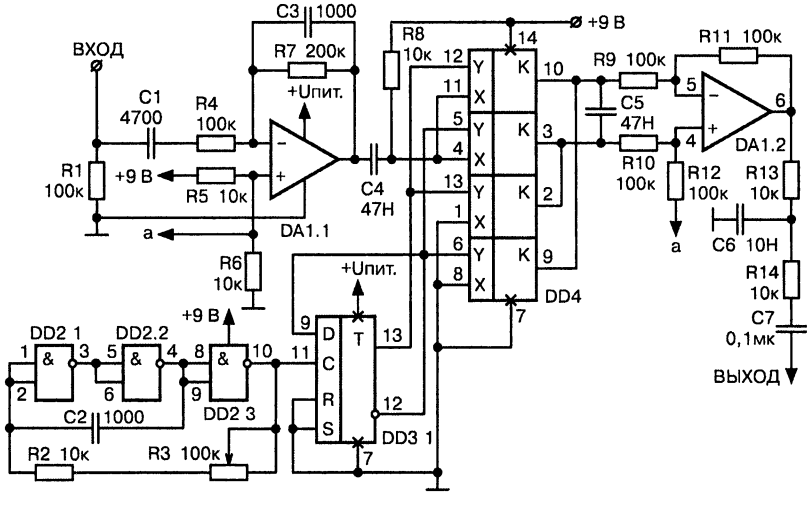


Рис. 10.23. Схема скремблера

Подстройка частоты тактовых импульсов, а следовательно частоты несущей, производится многооборотным резистором R3.

В пределах полосы частот 300—3000 Гц разборчивость речи после двух преобразований составляет не менее 65%.

Методы маскировки речи

Источник. При защите телефонных разговоров на энергетическом уровне осуществляется подавление электронных устройств перехвата информации с использованием активных методов и средств, отмечается на http://www.raksa.ru/about/material/news39.php.

К основным методам относятся:

- «синфазной» низкочастотной маскирующей помехи;
- высокочастотной маскирующей помехи;
- «ультразвуковой» маскирующей помехи;
- низкочастотной маскирующей помехи;
- повышения напряжения;
- понижения напряжения;
- компенсационный;
- «выжигания».

Метод «синфазной» маскирующей низкочастотной помехи используется для подавления электронных устройств перехвата речевой информации, подключаемых к телефонной линии последовательно в разрыв одного из проводов или через индукционный датчик к одному из проводов.

Суть метода заключается в подаче во время разговора в каждый провод телефонной линии согласованных по амплитуде и фазе относительно нулевого провода электросети 220 В маскирующих помеховых сигналов речевого диапазона частот (маскирующего низкочастотного шума).

Вследствие согласования по амплитуде и фазе в телефонном аппарате, подключаемом параллельно телефонной линии, эти помеховые сигналы компенсируют друг друга и не приводят к искажению полезного сигнала, т. е. не ухудшают качество связи.

Это интересно знать.

В любых устройствах, подключаемых к одному телефонному проводу (как последовательно, так и через индукционный датчик),

помеховый сигнал не компенсируется и «накладывается» на полезный сигнал.

А так как его уровень значительно превосходит полезный сигнал, то перехват передаваемой информации становится невозможным. В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные М-последовательности импульсов) в диапазоне частот от 100 до10000 Гц.

Метод высокочастотной маскирующей помехи заключается в подаче во время разговора в телефонную линию маскирующего помехового сигнала в диапазоне высоких частот звукового диапазона (маскирующего высокочастотного шума).

Частоты маскирующих помеховых сигналов подбираются таким образом, чтобы после прохождения низкочастотного усилителя или селективных цепей модулятора телефонной закладки их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии), но в то же время чтобы они не ухудшали качество связи.

Это интересно знать.

Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал.

Обычно используются частоты в диапазоне от 6—8 кГц до 12—16 кГц.

Для исключения воздействия маскирующего помехового сигнала на качество связи в устройстве защиты, подключаемым параллельно в разрыв телефонной линии, устанавливается **специальный фильтр нижних частот** с граничной частотой выше 3,4 кГц. Он подавляет (шунтирует) помеховые сигналы высокой частоты (не пропускает их в сторону телефонного аппарата) и не оказывает существенного влияния на прохождение низкочастотных речевых сигналов.

В качестве маскирующего шума используются широкополосные аналоговые сигналы типа «белого шума» или дискретные сигналы типа псевдослучайной последовательности импульсов с шириной спектра не менее 3—4 кГц.

Данный метод используется для подавления практически всех типов электронных устройств перехвата речевой информации, под-

ключаемых к телефонной линии как последовательно, так и параллельно. Однако эффективность подавления средств съема информации с подключением к линии последовательно (особенно при помощи индукционных датчиков) значительно ниже, чем при использовании метода «синфазной» маскирующей низкочастотной помехи.

Метод «ультразвуковой» маскирующей помехи в основном аналогичен рассмотренному выше. Отличие состоит в том, что частота помехового сигнала находится в диапазоне от 20—30 кГц до 50—100 кГц, что намного упрощает схему устройства подавления, но при этом эффективность данного метода по сравнению с методом высокочастотной маскирующей помехи ухудшается.

Метод низкочастотной маскирующей помехи. При использовании этого метода в линию при положенной телефонной трубке подается маскирующий низкочастотный помеховый сигнал. Этот метод применяется для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки (заполнению-памяти) в режиме записи шума, то есть при отсутствии полезного сигнала.

Метод повышения напряжения заключается в «поднятии» напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных закладок за счет перевода их передатчиков в нелинейный режим работы.

Повышение напряжения в линии до 25—35 В вызывает у телефонных закладок с последовательным подключением и параметрической стабилизацией частоты передатчика «уход» несущей частоты и ухудшение разборчивости речи.

У телефонных закладок с последовательным подключением и кварцевой стабилизацией частоты передатчика наблюдается уменьшение отношения сигнал/шум на 3—10 дБ. Передатчики телефонных закладок с параллельным подключением к линии при таких напряжениях в ряде случаев просто отключаются.

Метод понижения напряжения предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод применяется для нарушения функционирования всех типов электронных устройств перехвата информации с контактным (как последовательным, так и параллельным) подключением к линии, используя ее в качестве источника питания.

Рассмотренные выше методы обеспечивают подавление устройств съема информации, подключаемых к линии только на участке от защищаемого телефонного аппарата до АТС. Для защиты телефонных линий используются устройства, реализующие одновременно несколько методов подавления.

Компенсационный метод используется для стеганографической маскировки (скрытия) речевых сообщений, передаваемых абонентом по телефонной линии. Данный метод обладает высокой эффективностью подавления всех известных средств несанкционированного съема информации, подключаемых к линии на всем участке телефонной линии от одного абонента до другого.

Суть метода заключается в следующем: перед началом передачи скрываемого сообщения по специальной команде абонента на приемной стороне включается генератор шума. Он подает в телефонную линию маскирующую шумовую помеху (как правило, «цифровой» шумовой сигнал) речевого диапазона частот, которая в линии «смешивается» с передаваемым сообщением.

Одновременно этот же шумовой сигнал («чистый» шум) подается на один из входов двухканального адаптивного фильтра. На другой вход этого фильтра поступает аддитивная смесь принимаемого речевого сигнала и маскирующего шума.

Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет скрываемый речевой сигнал (передаваемое сообщение). Наличие таких устройств защиты у обоих абонентов позволяет организовать полудуплексный закрытый канал связи.

Метод «выжигания» реализуется путем подачи в линию высоковольтных (напряжение более 1500 В) импульсов, мощностью 15—50 ВА. Это приводит к электрическому «выжиганию» входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

Подача высоковольтных импульсов осуществляется при отключении телефонного аппарата от линии. При этом для уничтожения параллельно подключенных устройств подача высоковольтных импульсов осуществляется при разомкнутой, а последовательно подключенных устройств — при «закороченной» (как правило, в телефонной коробке или щите) телефонной линии.

ГЛАВА 11

ОБЗОР РЕСУРСОВ СЕТИ ИНТЕРНЕТ

Благодаря общедоступности сети Интернет в настоящее время сняты большинство проблем доступа к технической, а также любой другой информации. Однако работа с ресурсами всемирной сети коренным образом отличается от использования книжных источников и требует своих навыков и инструментов, а также везения.

Как искать в Интернете, чтобы найти

Огромным плюсом является наличие разнообразных поисковых систем как общей направленности (**Google**, **Yandex** и другие), так и порталов, архивов, поисковых машин специализирующихся на схемотехнике и электронике (**www.rlocman.com.ru**, **www.alldatasheet.com**, **www.radiofan.ru**, **www.allshemes.com**, **www.datasheetarchive.com** и т. п.). Благодаря такой поддержке нахождение необходимой информации кажется вопросом пяти минут.

Но тут есть свои подводные камни. Популярность ресурса у поисковой системы совсем не означает, что там имеется полная и доступная для ознакомления и использования информация. В большинстве случаев это может говорить о грамотной политике владельца сайта в плане оформления, на которое клюют поисковые машины. И на ничего не подозревающего, жаждущего знаний посетителя обрушится лавина ненужной рекламы.

В связи с существующим хаосом Интернет все еще остается неисследованным и загадочным местом, где через несколько ссылок с сайта на сайт можно попасть на оазис бесплатной и полной информации (программного обеспечения, схем, справочников).

Не стоит просто сохранять ссылку на найденные богатства. Бесценный оазис может через непродолжительное время также загадочно исчезнуть, как и появился. Поэтому все эксклюзивное, нигде не встреченное, то что вы так долго искали, должно быть тут же скопировано и сохранено.

Еще одной специфичной особенностью всемирной сети является то, что информация там размещена более чем в 90% случаев не теми людьми, которые ее создали. Поэтому зачастую принципиальные схемы, справочные данные, конструкции не имеют внятного описания (а то и выложивший их честно признается, что не знает, что это такое и для чего предназначено).

Подобное представление информации мало подходит для использования в качестве учебного пособия или руководства по изготовлению, но вполне годится для ознакомления с новыми направлениями, идеями и просто как руководство к действию.

Самым легким путем для поиска необходимой схемы будет задать ее название в окне популярного поисковика, например, «принципиальная схема эхолота». В результате мы получим ряд ссылок подходящих для знакомства с требуемыми принципиальными схемами десятилетней давности. Более современные схемы, видимо, обладают коммерческой ценностью, и для их поиска такой метод не очень хорош.

Если захочется глубже познакомиться с вопросом, следует найти специализированные схемотехнические сайты (через те же поисковики или по ссылкам одних ресурсов на другие), и поискать уже на страницах этих сайтов. Так как названия даже самых простых схем по воле автора (или оформителя) могут быть самыми невероятными как в плане имени, так и в плане грамматики, то в пределах сайта искать эффективнее вручную.

Кто же захочет узнать самые свежие и оригинальные веяния и идеи, тому прямой путь на **форумы специализированных сайтов**. Крупными буквами на входе форумов, как правило, написано: «Прежде чем задать вопрос, попробуй использовать поиск!» (то есть встроенный поиск по форуму). Это иногда помогает. Хотя **ручной поиск** по форумам наиболее результативен, он является самой неблагодарной деятельностью. Приходится справляться с подачей информации людьми самых разных возрастных групп, образования и мировоззрения. Нужная ссылка в форуме многолетней давности может уже давно не существовать, советчики могут непринужденно отослать на иноязычный сайт (и не всегда хотя бы англоязычный).

Но тем приятнее найти искомое в длиной цепочке догадок и запросов, когда читающий форум профессионал (или более удачливый энтузиаст) не смилостивится и поделится знанием или необходимой ссылкой.

Описанные ниже сайты, на мой взгляд, представляют собой одни из немногочисленных оазисов поддерживаемых уже достаточно дол-

гое время железными энтузиастами, добродушными спонсорами или дальновидными кураторами, где можно перевести дух и найти интересную и необходимую информацию без бесконечного перепрыгивания с ресурса на ресурс.

Популярные радиотехнические сайты

Российский сайт www.vrtp.ru. Как правило, схемотехнические сайты охватывают все направления схемотехники. Тема специальных технических средств присутствует на них в числе многих других тем. Российский сайт **www.vrtp.ru** (сокращение от **Very Reasonable Technological Pages**) является ярким исключением из этого правила, поскольку целиком посвящен теме всяческих шпионских технологий.

Это интересно знать.
*По своему наполнению, скорости поступления новых материалов ресурс **www.vrtp.ru** является наилучшим как среди отечественных, так и среди зарубежных сайтов.*

По поводу **зарубежных сайтов** надо отметить, что интересная схемотехника там появляется нечасто, видимо в связи с их коммерческой направленностью. Зарубежные схемы рассчитаны часто совсем для начинающих в качестве учебных пособий. Иногда можно отыскать схемы на специализированных элементах, которые у нас редкость.

Команда энтузиастов **www.vrtp.ru** постоянно развивает способы поддержания популярности ресурса, любой автор там может разместить свои изыскания. В связи с этим на сайте можно встретить как перерисованную откуда-нибудь коммерческую или профессиональную разработку, так и вполне работоспособную поделку студента или школьника.

Это интересно знать.
Если необходимы новые идеи, ссылки или информация о существующей «шпионской» схемотехнике — это то место откуда следует начать поиск (и, как правило, там же и закончить). Любую из опубликованных схем можно обсудить на форуме или снять возникшие вопросы прочтением уже имеющейся ленты обсуждений.

Еще один примечательный сайт «**Специальные радиосистемы**» — **www.radioscanner.ru**. Тут можно ознакомиться с описаниями распределения диапазонов частот, методами использования радиоприемной и радиопередающей техники, существующими радиосигналам в эфире, а также антенному хозяйству.

Это интересно знать.
Сайт больше примечателен не представленной схемотехникой, а отражением жизни радиоэфира, причем не радиолюбительского, а используемого различными ведомствами и службами.

Следует также отметить хорошую подборку законодательных документов регламентирующих использование приемопередающей и другой специальной техники.

Сайт также относится к специализированным и не распыляется на посторонние темы. Посетителями, как правило, являются или продвинутые любители, или профессионалы, не утратившие интереса к возне с техникой и радиоэфиром.

Следующий вид радиосайтов представляет собой **порталы схемотехники и справочной информации**. Среди Российских сайтов в этой категории наиболее заметен **www.kazus.ru**. На нем можно найти невообразимое множество отечественных и зарубежных схем, в том числе по шпионской тематике, разнообразную справочную информацию, ссылки, программное обеспечение — при умеренном засилье рекламы.

Уже долгое время успешно развивается сайт Александра Большакова «Радиофанат» **www.rf.atnn.ru** — он примечателен огромным объемом качественной схемотехники, отличным оформлением и большим количеством полезной сопутствующей информации. Раздел шпионской техники на этом сайте также заслуживает внимания.

Имеют широкую подборку различных конструкций **архивы схемотехники**:

- «Схема» — **www.shema.ru**;
- «Дайджест радиосхем» — **www.shems.h1.ru/?razd-ohrana.php**;
- «Радионет» — **www.radionet.com.ru/schem**;
- «Паяльник» — **http://www.cxem.net/**.

А также довольно интересные англоязычные архивы схем:

- http://www.discovercircuits.com/list.htm;
- http://www.uoguelph.ca/~antoon/circ/circuits.htm;
- http://www.electronics-lab.com/projects/rf/index.html.

Каждый из этих архивов имеет свою подборку шпионских штучек.

Отдельного внимания заслуживают **ресурсы любителей КВ и УКВ радиосвязи**. Вследствие большой и славной истории развития этого вида увлечения и спорта связисты гораздо лучше организованы, и, как правило, значительно лучше подкованы теоретически и практически, что и отражается на их Интернет-ресурсах.

Этих ресурсов существует множество во всех странах мира. Примером подобного Российского сайта могут служить:

- Сервер радиолюбителей России — **www.qrz.ru**;
- Сервер Кубанских радиолюбителей — **www.cqham.ru**.

Достаточно открыть один из подобных сайтов, и вы сможете по ссылкам обойти их все. Хотя и большая часть наполнения этих сайтов посвящена любительской радиосвязи, в то же время там можно разыскать: первоклассные индикаторы поля; конструкции антенн и их расчет; схемы радиоприемных и передающих устройств любых диапазонов; схемотехнику от ламповой до построенной на специализированных микросхемах.

Замечу, что вся эта информация приведена с грамотными обозначениями и описаниями.

Возможно, на момент выхода этой книги уже появились более продвинутые и наполненные ресурсы. Схемотехника меняется вслед за развитием элементной базы. Развиваются компьютерные методы разработки и анализа электронных схем.

Однако, чтобы использовать все современные достижения электроники и радиотехники, до сих пор необходимо и интересно многое паять, конструировать вручную. Чем более продвинутыми становятся радиоэлементы, тем интереснее получаются результаты.

СПИСОК ЛИТЕРАТУРЫ

Адрианов В.И. Бородин В.А. Соколов А.В. Шпионские штучки и устройства для защиты обьектов и информации. Справочное пособие. — СПб: Лань. — 1996.

Балахничев И.Н. Дрик А.В. Коммерческие электронные схемы. — Минск: Битрикс. — 1997.

Балахничев И.Н. Дрик А.В. Практическая телефония. — Минск: Наш город. — 1998.

Балахничев И.Н. Ровдо А.В. Дрик А.В. Экспериментальная электроника. — Минск: Битрикс. — 1999.

Белолапотков В. Г., Семьян А. П. 500 схем для радиолюбителей. Шпионские штучки и не только... — Изд. 2-е, перераб. и доп. — СПб.: Наука и техника. — 2008.

Бондарев В. Рукавишников А. Применение микросхемы К174ПС1. — Радио, №2. — 1989. — С. 55.

Василев Живко Млад. — ЧМ микропередатчик. — Конструктор, №1. — 2000. — С. 19.

Виноградов Ю. Датчик вибрации для охранного устройства. — Радио, № 12. — 1994. — С. 38 .

Виноградов Ю. ИК линия связи в охранной сигнализации. Радио, 1998 №2, С.50.

Горланд Раджик Простейший ЧМ приемник. — Electronics World incorporating Wireless World, №4. — 2000. — С. 300.

Граф Р.Ф. Шните В. Энциклопедия электронных схем. Том 7, часть 2. — М.: ДМК. — 2000.

Гутников В.С. Интегральная электроника в измерительных устройствах, 2-е изд., перераб. и доп. — Л.: Энергоатомиздат. — 1988.

Исаев А. СВЧ датчик движения для охранной сигнализации. (Электроника в быту). — Радио, № 12. — 2002. — С. 41.

Койнов А. Ультразвуковое охранное устройство. — Радио, № 7. — 1998.

Корякин-Черняк С. Л. Квартирный вопрос. — СПб.: Наука и техника. — 2009.

Корякин-Черняк С. Л. Шпионские штучки своими руками. — СПб.: Наука и техника. — 2012.

Крупа А., Балахничев И.Н., Дрик А. В. Борьба с телефонным пиратством. — Минск: Битрикс. — 1999.

Нечаев И. Звуковое сопровождение без проводов. — Радио, №10. — 1998.

Операционные усилители и компараторы. — М.: Издательский дом «Додэка». — 2001.

Пейтон А. Волш В. Аналоговая электроника на операционных усилителях. Пер. с англ. — М.: БИНОМ. — 1994.

Радиоприемные устройства. *Под ред. А.П. Жуковского.* — М.: Высшая школа. —1989.

Ред Э. Справочное пособие по высокочастотной схемотехнике: схемы, блоки, 50-омная техника. Пер с нем. — М.: Мир. — 1990.

Соколов А. В. Шпионские штучки. Новое и лучшее. — СПб.: Полигон. — 2000.

Уваров А. С. Устройство для снятия информации со стекла. — Радиоконструктор, №3. — 2001. — С. 24.

Федоров В. СВЧ делитель для частотомера. — Радиолюбитель, №3. — 2000. — С. 33.

Фролов Е. (UA3ICO) *Доломанов В.* (UA3IBT) *Березкин Н.* (UA3JD). УКВ ЧМ приемник на 145 МГц. — Радио, № 3. — 1991. — С. 22—25.

Чистов В. Детектор радиоволн. — Радио, № 10. — 1998. — С. 53.

Шелестов И.П. Радиолюбителям — полезные схемы. Часть 3. — М: СОЛОН-Р. — 2003.

Шило В.Л. Популярные цифровые микросхемы: Справочник. — М.: Радио и связь. — 1988.

LT1083/84/85 Fixed 3A, 5A, 7.5A Low Dropout Positive Fixed Regulators © LINEAR TECHNOLOGY CORPORATION. — 1994.

Philips Semiconductors Product specification. Sensitive 1 GHz divide-by-64/divide-by-256 switchable prescaler SAB6456, SAB6456T.

Planet microchip. July 1999 Technical Library CD-ROM. Microchip Technology Inc.

СПИСОК РЕСУРСОВ ИНТЕРНЕТ

http://bezpeka.desant.com.ua
http://braincambre500.frecservers.com
http://cadlab.ru
http://ciscom.ru
http://cxem.net
http://cxem.net/
http://cxema.3dn.ru/
http://electricalschool.info/
http://electrik.info/
http://electronic.vladbazar.com\
http://elektronicspy.narod.ru
http://irls.narod.ru
http://irls.narod.ru/
http://irlx.narod.ru/
http://isinpol.net
http://kazus.ru
http://leg ion-33/Sxemy/
http://microcopied.ru/content
http://mirknig.com/index.php?do=search
http://mods.radioscanner.ru
http://newsrack.ru/content
http://pk.altnet.ru
http://radiolla.narod.ru
http://radiomaster.com.ua
http://radiopartal.tut.su/
http://roma.3dn.ru
http://shema.org.ua
http://shemotehnik.ru/
http://sima0607.se-ua.net
http://spying.by.ru
http ://vesh.ua
http://web.geowap.mobi/shemes.html
http://www.cqham.ru/
http://www.qrz.ru/
http://www.radioland.net.ua/
http://www.radioman.ru/shem/
http://www.radio-portal.ru/
http://www.radioradar.net/about_project/index.html
http://www.radiosait.ru/
http://www.z-oleg.com/
ra4a.narod.ru/portal/Sprawka.html
ru3ga.qrz.ru/file.shtml
schematic.by.ru/
umup.narod.ru/
valvol.nightmail.ru/books.html
www.1el.ru/
www.alldatasheet.com
www.allshemes.com
www.avr.nikolaew.org
www.bvn123.narod.ru
www.chertezhi.ru/
www.compradio.nm.ru
www.cqham.ru
www.cqham.ru/lib.htm
www.datasheetarchive.com
www.discovercircuits.com
www.efo.ru/cgi-bin/go?732
www.electronic-circuits-diagrams.com
www.electronics-diy.com
www.electronics-lab.com
www.electroscheme.ru
www.elremont.nm.ru/
www.flexi-spy.ru
www.general.pop3.ru
www.go.elec.ru/
www.guarda.ru
www.imagineeringezine.com
www.irls.narod.ru
www.kazus.ru
www.krs.poltava.ua
www.kruso.narod.ru/poiskk.htm
www.lamaster.ru/
www.master-tv.com
www.nnov.rfnet.ru
www.qrz.ru
www.qsl.net
www.radiofan.ru
www.radiofan.ru
www.radioland.net.ua
www.radiomaster.net
www.radiomaster.net/index.php
www.radionet.com.ru
www.radiopirat.h11.ru/pic/index.htm
www.radioscanner.ru
www.radio-portal.ru
www.raksa.ru
www.rf.atnn.ru
www.rlocman.com.ru
www.rlocman.ru/
www.shema.ru
www.shematic.net
www.shems.h1.ru
www.softsklad.ru/science/spravs/5programs2.html
www.spyline.ru
www.spystuff.pdf
www.tstu.ru/r.php?r=education.clib&id=12
www.uni-electronics.newmail.ru
www.uoguelph.ca
www.valtar.ru/encyclop.htm
www.vrtp.ru