КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Книга 26

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 26

А. В. ТЕЛЬНЫЙ Ю. М. МОНАХОВ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики

Учебное пособие

Под редакцией профессора М. Ю. Монахова

Электронное издание

Владимир 2018

ISBN 978-5-9984-0875-5

УДК 004.056.53
ББК 32.81

Редактор серии – профессор М. Ю. Монахов

Рецензенты:

Доктор технических наук, профессор
зав. кафедрой вычислительной техники и систем управления
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
В. Н. Ланцов

Кандидат технических наук
зам. руководителя РАЦ ООО «ИнфоЦентр»
Н. В. Вертилевский

Тельный, А. В. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ : Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики : учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2018. – 161 с. – (Комплексная защита объектов информатизации. Кн. 26). – ISBN 978-5-9984-0875-5. – Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Acrobat Reader; дисковод CD-ROM; 3,20 Мб. – Загл. с титула экрана.

Представлена 26-я книга из серии «Комплексная защита объектов информатизации». В пособии излагается систематизированный материал по первой части учебного курса «Техническая защита информации» – основные понятия, термины, определения и характеристики технических каналов утечки информации и средств защиты информации от утечки по техническим каналам.

Предназначено для студентов вузов, обучающихся по направлению 10.03.01 «Информационная безопасность» и специальности 10.05.04 «Информационно-аналитические системы безопасности».

Ил. 43. Табл. 29. Библиогр.: 50 назв.

УДК 004.056.53
ББК 32.81

ISBN 978-5-9984-0875-5

ВВЕДЕНИЕ

В современном обществе проблема обеспечения конфиденциальности информации, защита информационных ресурсов от зарубежных разведок, конкурентов, преступных сообществ, организаций, групп, формирований и противозаконной деятельности отдельных лиц становится все более и более актуальной.

В последнее время активное развитие получила конкурентная разведка для получения экономического преимущества перед конкурентами. Получение конфиденциальной информации при проведении законных и незаконных разведывательных мероприятий становится важнейшим условием достижения коммерческого успеха.

В условиях рыночной экономики масштабы промышленного шпионажа резко возрастают. Все шире используются самые современные технические достижения в сфере разработки и использования несанкционированного доступа к конфиденциальной информации.

Однако в сложившихся условиях развиваются и совершенствуются технические средства защиты информации от утечек по техническим каналам. На современном рынке представлен арсенал самых современных технических средств, способных обеспечить надежную защиту информационных ресурсов и телекоммуникационных систем от утечки информации при использовании визуально-оптических, телевизионных, инфракрасных, акустических, радио-, радиотехнических и других средств разведки.

Для обеспечения защиты конфиденциальной информации необходимо знать возможности технических средств разведки, способы их применения, и технические каналы, по которым ценная информация потенциально может быть перехвачена.

В предлагаемом учебном пособии даны классификация и характеристики технических каналов утечки информации, обрабатываемой техническими средствами, передаваемой по каналам связи, а также акустической, видовой и материально-вещественной информации.

Рассмотрены основные технические показатели и характеристики каналов связи, методология и способы несанкционированного съема информации с объектов разведки, подробно рассмотрены основные показатели и характеристики технических средств защиты информации от утечки по техническим каналам. В приложениях к пособию приведены сводные характеристики устройств несанкционированного съема информации по различным физическим каналам утечки.

Пособие предназначено в первую очередь для студентов и аспирантов, специализирующихся в вопросах комплексной защиты объектов информатизации, и может быть полезным в системе переподготовки и повышения квалификации инженерно-технических кадров. Для более углубленного изучения данной предметной области приводится библиографический список литературы.

ГЛАВА 1. ОБЩАЯ КЛАССИФИКАЦИЯ ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛОВ СВЯЗИ

Канал связи (англ. channel, data line) — система технических средств и среда распространения сигналов для односторонней передачи данных (информации) от отправителя (источника) к получателю (приёмнику). Канал связи является составной частью канала передачи данных. Общая схема канала связи представлена на рис.1.

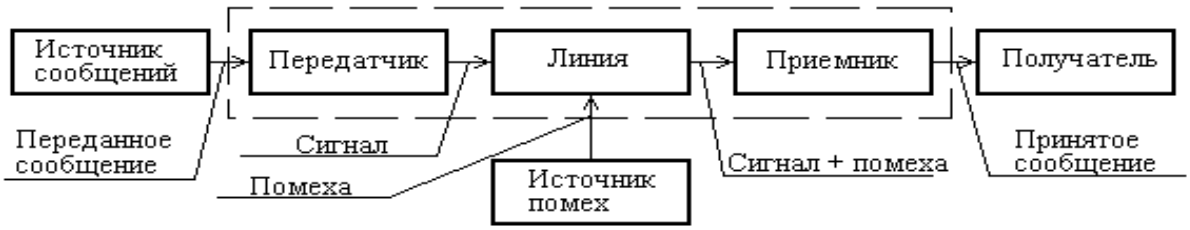


Рис.1. Общая схема канала связи

Классификация каналов связи

1. Классификация каналов по типу среды распространения. Каналы связи делятся на проводные, акустические, оптические, инфракрасные и радиоканалы [1-7].

Проводные каналы связи. Воздушные, кабельные и др. проводные каналы это электрические провода (например, телефонные линии, линии широкополосного радиовещания, оповещения, линии систем сигнализации, СКУД и прочие инженерные системы зданий и передачи данных, линии электропередачи и др), кабели (витая пара (группы скрученных проводов) – высокочастотные, радиочастотные кабели), волноводы и микрополоски [1-4]. Кабели витой пары (UTP и FTP) применяют в локальных вычислительных сетях и системах передачи данных, IP-телефонии. Радиочастотные кабели применяют в телевизионном оборудовании, кабельном телевидении, в межблочных соединениях радиотехнических систем. Волноводы и микрополоски применяют в технике СВЧ.

Акустические каналы связи [1-4] используются для передачи семантической информации между субъектами (людьми) или используют специальные звуководы (обычно как составные части стетоскопов и фонедоскопов). Акустические каналы используются для связи под водой между морскими объектами и для ориентации под водой (ультразвуковая эхолокация). Подводный акустический канал ведет себя как многопутевой канал благодаря переотражениям от поверхности и дна моря.

Оптические каналы связи. Наиболее перспективным является использование волоконно-оптических кабелей. В волоконно-оптический кабеле носителем информации является пульсирующий световой луч, распространяемый по стекловолокну. Световые лучи имеют значительно большую полосу частот, чем электрические волны, и скорость передачи информации может достигать сотен Мбит/с, а теоретический предел скорости передачи световодных каналов - десятки триллионов бит/с. Волоконно-оптический кабель состоит из отдельного стекловолокна, содержащего жилу световода и оболочку с разными показателями преломления $n1$ и $n2$.

Кроме того, этот кабель имеет еще защитную внешнюю оболочку, которая экранирует световод от внешних (фоновых) засветок. Различают одномодовое и многомодовое. Многомодовое и одномодовое оптоволокно отличаются в размерах сердечника световода и в соответствии с этим способом распространения оптического излучения в волокне. Оптоволокно имеет два концентрических слоя: внутренний, называемый сердцевиной (core), и внешний (cladding). Оба слоя состоят из материалов с разными показателями преломления (коэффициент преломления внешнего слоя примерно на 1% меньше коэффициента преломления сердцевины). Свет, направляемый в волокно, распространяется в нем за счет многократного отражения на границе сердцевина-внешний слой. Термин "одномодовый" означает, что такой тонкий сердечник может передавать только один световой несущий сигнал (или моду).

Инфракрасные каналы связи. В настоящее время используются БОКСы (беспроводные оптические каналы связи при максимальном удалении между "точками" до 1 км) для организации соединения отдельных ЛВС, а также релейной связи с использованием оптических линий, работающих в инфракрасном участке спектра [1-2].

Радиоканалы. Радиоканалы классифицируются в первую очередь по частоте излучения [3-4]. Классификация диапазонов радиоволн представлена в таблице 1.

Таблица 1

Классификация радиочастот по международному регламенту радиосвязи

Классификация радиочастот по международному регламенту радиосвязи				
Длина волны	**Название диапазона**	**Частота полосы**	**Название полосы**	**Применение**
100000 км – 10000 км	Декамегаметровые	3-30Гц	Крайне низкие (КНЧ; ELF)	Связь с подводными лодками, геофизич. исследования
10000 км – 1000 км	Мегаметровые	30-300 Гц	Сверхнизкие (СНЧ; SLF)	Связь с подводными лодками, геофизические исследования
1000 км – 100 км	Гектокилометровые	300-3000 Гц	Инфранизкие (ИНЧ; ULF)	
100 км – 10 км	Мериаметровые	3 – 30 кГц	Очень низкие (ОНЧ; VLF)	Связь с подводными лодками
10 км – 1 км	Длинные волны километровые	30 – 300 кГц	Низкие (НЧ; LF)	Радиовещание, радиосвязь
1 км – 100 м	Средние волны Гектометровые	300 – 3000 кГц	Средние (СВ; MF)	Радиовещание, радиосвязь
100 м – 10 м	Короткие волны Декаметровые	3 – 30 мГц	Высокие (ВЧ; HF)	Радиовещание, радиосвязь, радиостанции
10 м – 1 м	Метровые волны	30 – 300 Мгц	Очень высокие (ОВЧ; VHF)	Телевидение; радиовещание, радиосвязь, радиостанции

Окончание таблицы 1

Длина волны	**Название диапазона**	**Частота полосы**	**Название полосы**	**Применение**
1 м – 100 мм	Дециметровые	300 – 3000 Мгц	Ультравысокие (УВЧ; UHF)	Телевидение, радиосвязь, мобильная связь, микроволновые печи, радиостанции
100 мм – 10 мм	Сантиметровые	3 -30 ГГц	Сверхвысокие (СВЧ; SHF)	Радиолокация, спутниковое телевидение, радиосвязь, беспровод-ные ССПД; спутниковая навигация
10 мм – 1 мм	Миллиметровые	30 – 300 ГГц	Крайне высокие (КВЧ; EHF)	Радиоастрономия, радиорелейная связь, радиолокация, метеорология
1мм – 0,1 мм	Децимиллимитровые	300 – 3000 ГГц	Гипервысокие частоты, длинноволновая область инфоракрасного излучения	Радиоастрономия, радиолокация, тепловизоры

Примеры выделенных радиодиапазонов [2;3;11] приведены в таблице 2.

Таблица 2

Примеры выделенных радиодиапазонов

Название	**Полоса частот**	**Длинна волны**
Диапазон средних волн с амплитудной модуляцией (АМ волны)	530-1610 кГц	656,646 – 186,206 м
Разные диапазоны коротких волн	5,9 – 26,1 Мгц	50,81 – 11,486 м
Гражданский диапазон КВ (любители)	26,965 – 27,405 Мгц	11,1178 – 10,9394 м
Телевизионные каналы 1-5	48-100 Мгц	6,246 – 2,998 м
Телевизионные каналы 6-12	174 – 230 Мгц	1,7229 – 1,30304 м
Телевизионные каналы 21-39	470 – 622 Мгц	6,3786- 4,8198 дм
Диапазон УКВ с частотной модуляцией (FM волны)	88-108 Мгц (в Японии 76 – 90 Мгц)	3,4 – 2,776м (в Японии 3,94–3,33м)

Диапазоны радиочастот в гражданской радиосвязи.

В России для гражданской радиосвязи выделены три диапазона частот: - 27 МГц (Си-Би, Citizens Band - гражданский диапазон), с разрешённой выходной мощностью передатчика до 10 Вт; - 433 МГц (LPD, Low Power Device), выделено 69 каналов для носимых радиостанций с выходной мощностью передатчика не более 0,01 Вт; - 446 МГц (PMR, Personal Mobile Radio), выделено 8 каналов для носимых радиостанций с выходной мощностью передатчика не более 0,5 Вт.

Некоторые частоты, используемые в гражданской авиации:
- 74,8 - 75,2 МГц - маркерные радиомаяки; - 108 - 117,975 МГц - радиосистемы навигации и посадки; - 118 - 135,975 МГц - УКВ-радиосвязь (командная связь);
- 328,6 - 335,4 МГц - радиосистемы посадки (глиссадный канал); - 960 - 1215 МГц - радионавигационные системы.
Диапазоны спутниковой связи:
- диапазон L Полоса частот в диапазоне 0.5 - 2 GHz, которая используется преимущественно для головой связи; - диапазон Ku Полоса частот в диапазоне 10.9 - 17 GHz, которая используется для стационарных услуг спутников; - диапазон Ka Полоса частот в диапазоне 18 - 31 GHz, которая используется для спутников во всем мире.
Диапазоны электромагнитных излучений [1-4] и их источники приведены в таблице 3.

Таблица 3

Диапазоны электромагнитных излучений и их источники

Название диапазона	**Длина волны**	**Частота**	**Источники**
Сверхдлинные радиоволны	более 10км	менее 30 кГц	Атмосферные явления, переменные токи в проводниках и колебательных контурах
Длинные радиоволны	10 км – 1км	30 кГц – 300 кГц	
Средние радиоволны	1 км – 100 м	300 кГц – 3 мГц	
Короткие радиоволны	100 м – 10 м	3 мГц – 30 мГц	
Ультракороткие радиоволны	10 м – 1 мм	30 мГц – 300 ГГЦ	
Инфракрасное излучение	1 мм – 780 нм	300 ГГЦ – 429 ТГц	Излучение молекул и атомов при тепловых и электрических воздействиях
Видимое оптическое излучение	780 нм – 380 нм	429 ТГц – 750 ТГц	
Ультрафиолетовое излучение	380 нм – 10 нм	$7{,}5x10^{14}$ Гц - $3x10^{16}$ Гц	Излучение атомов под воздействием ускоренных электронов
Рентгеновское излучение	10 – $5x10^{-3}$ нм	$3x10^{16}$ Гц - $6x10^{19}$ Гц	Атоиные процессы при воздействии ускоренных заряженных частиц
Гамма излучение	менее $5x10^{-3}$ нм	более $6x10^{19}$ Гц	Ядерные и космические процессы, радиоактивный распад

Беспроводные (радиоканалы наземной и спутниковой связи) каналы передачи данных

- Радиоканалы наземной (радиорелейной и сотовой) и спутниковой связи.

- Радиорелейные каналы передачи данных. Радиорелейные каналы связи состоят из последовательности станций, являющихся ретрансляторами. Связь осуществляется в пределах прямой видимости, дальности между соседними станциями - до 50 км.

- Спутниковые каналы передачи данных.

- Сотовые каналы передачи данных. Сотовая связь - это беспроводная телекоммуникационная система, состоящая из сети наземных базовых приемо-передающих станций и сотового коммутатора (или центра коммутации мобильной

связи). Стандарты сотовой связи [34;36] (таблица 4): 1G. NMT - Nordic Mobile Telephony; 1G. AMPS - Advanced Mobile Phone Service; 2G. DAMPS - Digital Advanced Mobile Phone System; 2G. CDMA One (IS-95); 2G. GSM - Global System for Mobile Communications; 3G. CDMA2000; 3G. UMTS - Universal Mobile Telecommunications System; 3G. TD-SCDMA - Time Division Synchronous Code Division Multiple Access; 4G. LTE - Long Term Evolution; 4G. Mobile WIMAX.

Таблица 4.

Поколения сотовой связи

Поколение	**2G**	**2,5G**	**3G**	**3,5G**	**4G**
Начало разработок	1980	1985	1990	<2000	2000
Реализация	1991	1999	2002	2006-2007	2008-2010
Сервисы	цифровой стандарт, поддержка коротких сообщений (SMS)	большая ёмкость, пакетная передача данных, увеличение скорости сетей второго поколения	ещё большая ёмкость, скорости до 2 Мбит/с	увеличение скорости сетей третьего поколения	большая ёмкость, IP-ориентированная сеть, поддержка мультимедиа, скорости до сотен мегабит в секунду
Скорость передачи	9,6-14,4 кбит/с	115 кбит/с (1 фаза), 384 кбит/с (2 фаза)	до 3,6 Мбит/с	до 42 Мбит/с	100 Мбит/с - 1 Гбит/с
Стандарты	TDMA, CDMA, GSM, PDC	GPRS, EDGE (2.75G), 1xRTT	WCDMA, CDMA2000, UMTS	HSDPA, HSUPA, HSPA, HSPA+	LTE-Advanced, WiMax Release 2 (IEEE 802.16m), WirelessMAN-Advanced
Сеть	PSTN	PSTN, сеть пакетной передачи данных	сеть пакетной передачи данных	сеть пакетной передачи данных	сеть пакетной передачи данных

- Радиоканалы передачи данных WiMAX (Worldwide Interoperability for Microwave Access) аналогичны Wi-Fi. WiMAX, в отличие от традиционных технологий радиодоступа, работает и на отраженном сигнале, вне прямой видимости базовой станции.

- Радиоканалы передачи данных MMDS (Multichannel Multipoint Distribution System). Эти системы способна обслуживать территорию в радиусе 50—60 км

- Радиоканалы передачи данных для локальных сетей. Стандартом беспроводной связи для локальных сетей является технология Wi-Fi.

802.11 Первый вариант стандарта, диапазон работы – 2.4 ГГц. Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. В настоящее время не используется. Ширина канала – 11МГц.

802.11a Стандарт, использующий диапазон 5ГГц, обеспечивает скорости работы 54 до 36, 24, 18, 12, или 6 Мбит/с. Ширина канала – 20МГц.

802.11b Дальнейшее развитие стандарта 802.11, использующего диапазон 2.4ГГц, Обеспечивает скорости работы 11, 5.5, 2 и 1 Мбит/с Ширина канала – 22МГц.

802.11g Наиболее распространенный стандарт, обеспечивающий лучшую по сравнению с 802.11b пропускную способность. Стандарт использует диапазон 2.4 ГГц, и обеспечивает скорости работы 54, 36, 24, 18, 12 и 6 Мбит/с. Обратно совместим со стандартом 802.11b, и, соответственно поддерживает также скорости работы 11, 5.5, 2 и 1 Мбит/с. Ширина канала – 20МГц.

802.11n Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 МБит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 480 Мбит/с. Устройства 802.11n работают в диапазонах 2,4 — 2,5 или 5,0 ГГц.

- Радиоканалы передачи данных Bluetooht - это технология передачи данных на короткие расстояния (не более 10 м) и может быть использована для создания домашних сетей. Скорость передачи данных не превышает 1 Мбит/с.

2. Классификация каналов по виду передаваемых первичных сигналов (сообщений). Каналы классифицируются на:

- телеграфные; - телефонные; - звукового вещания; - телевизионные; - передачи данных и др.

Кроме того, при классификации разделяют аналоговые; цифровые; импульсные, пакетные, шумоподобные и др. сигналы

3. Классификация каналов по характеру сигналов на входе и выходе канала. Каналы классифицируются на:

- дискретные (на входе и выходе канала действуют дискретные сигналы);
- непрерывные (аналоговые) (на входе и выходе канала действуют непрерывные (по уровням) сигналы);
- дискретно-непрерывные или непрерывно-дискретные (на входе канала действует дискретный сигнал, а на выходе – непрерывный (по уровням) или наоборот).

4. Классификация каналов по видам параметров.

Каналы связи могут быть линейными и нелинейными, временными и пространственно-временными. Системы передачи информации бывают одноканальными и многоканальными. Если система связи построена на однотипных каналах связи, то ее название определяется типовым названием каналов. В противном случае используется детализация классификационных признаков.

5. Классификация каналов по режимам и правилам приёма и передачи информации.

По указанным признакам каналы связи делят на симплексные, полудуплексные и дуплексные. Симплексный канал связи — это односторонний канал, данные по нему

могут передаваться только в одном направлении. Первый узел способен отсылать сообщения, второй может только принимать их, но не может подтвердить получение или ответить. Типичным примером полудуплексного канала связи является радио и телевидение.

При полудуплексном типе связи оба абонента имеют возможность принимать и передавать сообщения. Каждый узел имеет в своём составе и приёмник, и передатчик, но одновременно они работать не могут. В каждый момент времени канал связи образуют передатчик одного узла и приёмник другого. Типичным примером полудуплексного канала связи является радиостанция.

По дуплексному каналу данные могут передаваться в обе стороны одновременно. Каждый из узлов связи имеет приёмник и передатчик. После установления связи передатчик первого абонента соединяется с приёмником второго и наоборот. Классическим примером дуплексного канала связи является телефонный разговор

6. Классификация каналов по способу передачи данных.

Асинхронная передача. При передаче данных отдельными байтами осуществляется только побитовая синхронизация, синхронизация по кадрам не ведется. Такой режим работы называется асинхронным или старт-стопным. Такой режим удобен при невысоком качестве канала связи (например, высокий уровень помех), при передаче информации от устройств, которые генерируют байты данных в случайные моменты времени. Так работает клавиатура дисплея или другого терминального устройства, с которого человек вводит данные для обработки их компьютером. Асинхронным описанный режим называется потому, что каждый принятый байт может быть смещен во времени относительно переданного байта на случайный промежуток времени. Это резко снижает требования к характеристикам системы передачи. Асинхронная передача является более простой, но заставляет сопровождать каждый байт сигналами "Старт - Стоп ", что снижает эффективность использования канала и, в конечном итоге, скорость передачи по каналу информационных битов.

Синхронная передача. При синхронном режиме передачи пользовательские данные собираются в кадр, который предваряется байтами синхронизации (на рис.3 - флаги). Старт-стопные биты между соседними байтами отсутствуют. Байт синхронизации - это байт, содержащий заранее известный код, например 0111110, который оповещает приемник о приходе кадра данных. Его обычно называютфлагом. При его получении приемник должен войти в байтовый синхронизм с передатчиком, то есть правильно понимать начало очередного байта кадра. Синхронная передача позволяет более эффективно использовать пропускную способность канала, но требует более сложной аппаратуры. Обычно она используется на хороших каналах для передачи данных с высокой скоростью - 64 кбит/с до 8192кбит/с и выше.

7. Классификация каналов по методам разделения канальных сигналов в многоканальных системах связи. Каналы классифицируются:

- с простейшими методами разделения (первичные сигналы передаются без каких-либо преобразований в исходном диапазоне частот). Различают:

- частотное разделение каналов (ЧРК) – FDMA. Данный метод стоится с применением многоканальных фильтров и преобразователей частоты;

- временное разделение каналов (ВРК) – TDMA;

- кодовое разделение каналов (КРК) – CDMA. Принцип кодового разделения каналов заключается в разделении каналов по кодам;

- спектральное разделение каналов (СРК) – WDMA. Принцип спектрального разделения заключается в разделение каналов по длине волны.

- с более совершенными методами разделения (первичные сигналы преобразуются в канальные, наделенные определенными отличительными признаками). Пример: с линейным разделением (разделяющие устройства являются линейными 4-полюсниками) (с временным разделением, с частотным разделением, с разделением по фазе, с разделением по форме); с нелинейным разделением (разделяющие устройства являются нелинейными 4-полюсниками) (с разделением по уровню, с комбинационным разделением) и др.

8. Классификация каналов по занимаемой полосе частот. Каналы классифицируются следующим образом:

- узкополосные (занимают узкую полосу частот). Пример: канал тональной частоты (300…3400 Гц) в телефонии;

- широкополосные (занимают широкую полосу частот, в них могут разместиться несколько узкополосных). Пример: канал передачи сигналов изображения телевидения (50…6500000 Гц);

- сверхширокополосные.

9. Классификация каналов по характеру эксплуатации. Каналы классифицируются на:

- выделенные, постоянно включенные между двумя пунктами;

- коммутируемые, создаваемые по вызову на основе разных каналов и распадающиеся автоматически после окончания передачи.

10. Классификация каналов по модуляции (манипуляции) сигналов в них. Классификация каналов по виду модуляции [4;10;11] представлена в таблице 5.

Таблица 5.

Типовые сокращения видов модуляции:

QPSK	квадратурная фазовая манипуляция
ADM	адаптивная дельта-модуляция
ADPCM	адаптивная дифференциальная импульсно-кодовая модуляция
ADSM	асинхронная сигма-дельта-модуляция
AFM	амплитудно-частотная модуляция
APCM	адаптивная импульсно-кодовая модуляция
APK	амплитудно-фазовая манипуляция (система манипуляции)
APM	амплитудно-фазовая модуляция
APSK	амплитудно-фазовая манипуляция
BCFSK	частотная манипуляция двоичным кодом
BDM	двоичная дельта модуляция

Продолжение таблицы 5

BDPSK	двоичная дифференциальная фазовая манипуляция
BFSK	двоичная частотная манипуляция
BPSK	двоичная фазовая манипуляция
C4FM	непрерывная четырёхуровневая частотная модуляция
CAP	амплитудно-фазовая модуляция без несущей
CASK M=16	когерентая амплитудная манипуляция
CASK M=2	когерентая амплитудная манипуляция однополярная
CDM	компрессированная дельта модуляция
CFM	компрессированная частотная модуляция
CFSK M=2, 4	когерентная частотная манипуляция
CIM	импульсно-кодовая модуляция
CPFSK	частотная манипуляция с непрерывной фазой
CPM	фазовая модуляция с непрерывной фазой
CPSK	когерентная фазовая манипуляция
CQPSK	когерентная четвертичная фазовая манипуляция
DDM	относительная дискретная модуляция
DECPSK	дифференциально-кодированная когерентная фазовая манипуляция
DEPSK	дифференциально-кодированная фазовая манипуляция
DFSK	двойная частотная манипуляция
DM	дельта модуляция
DMT	многотоновая модуляция (Дискретный мультитон)
DPCM	дифференциальная импульсно-кодовая модуляция
DPCM	дельта импульсно-кодовая модуляция
DPM	дифференциальная фазовая модуляция
DPPM	дифференциальная импульсно-позиционвая модуляция
DPSK 2(4,8,16)	дифференциальная фазовая манипуляция
DQPSK	дифференциальная QPSK (см. QPSK)
FFSK	фильтруемая частотная манипуляция
FM	частотная модуляция
FMFB	частотная модуляция с обратной связью
FM-PM	частотно-фазовая модуляция

Продолжение таблицы 5

FSK	частотная манипуляция
GFPM	частотно-позиционная модуляция со стробированием
GMSK	минимальная манипуляция с гауссовым фильтром или гауссовская минимальная манипуляция
GTFM	«прирученная» частотная модуляция
HADM	гибридная аналогово-цифровая модуляция
HM	гибридная модуляция или фоновая модуляция
LDM	линейная дельта-модуляция
LPCM	линейная импульсно-кодовая модуляция
MFKP	многочастотная манипуляция
MFSK	многократная или многоуровневая частотная манипуляция
MPSK	многократная фазовая манипуляция
MSK	минимальная манипуляция
NBFM	узкополосная частотная модуляция
NCASK M=2	некогерентая амплитудная манипуляция
PAM	амплитудно-фазовая модуляция, амплитудно-импульсная модуляция АИМ
PBM	пакетно-импульсная модуляция
PCM-FM	ИКМ-ЧМ (импульсно-кодовая модуляция)
PDBM	двоичная фазо-импульсная модуляция
PDM-FM	ШИМ-ЧМ (широтно-импульсная модуляция)
PFM	ЧИМ (частотно-импульсная модуляция)
PFSK	частотно-фазовая манипуляция
PHDM	фазо-разностная модуляция
PIM	ФИМ (фазо-импульсная модуляция)
PM	фазовая модуляция
PNM	импульсно-числовая модуляция
PPBM	двоичная поляризационно-импульсная модуляция
PPM	фазо-импульсная модуляция
PRM	ЧИМ (частотно-импульсная модуляция)
PSK	фазовая манипуляция

окончание таблицы 5

PTM	ШИМ и фазо-временная модуляция
QM	квадратурная модуляция
QPAM	АИМ с квантованием
QPSK	квадратурно-фазовая манипуляция
QPSK	четвертично-фазовая манипуляция
RPSK	относительная фазовая манипуляция
SDM	статистическая дельта модуляция
SFM	ЛЧМ и пространственная частотная модуляция
SSM	модуляция с расширенным спектром
SSPSK	фазовая манипуляция с расширенным спектром
TFM	управляемая частотная модуляция
WBFM	широкополосная частотная модуляция

11. Классификация каналов по топологии сетей связи. Каналы классифицируют по топологии:

- общая шина; - кольцевая; - звездообразная или радиальная; - полносвязная топология; - древовидная иерархическая или узловая топология и пр.

12. Классификация каналов по способам защиты передаваемой информации. Каналы классифицируют: - каналы с открытой связью; - каналы с закрытой связью (конфиденциальная или засекреченная).

13. Классификация каналов по степени автоматизации информационного обмена. Каналы классифицируют на: - неавтоматизированные — управление радиостанцией и обмен сообщениями выполняется оператором; автоматизированные — вручную осуществляется только ввод информации; - автоматические — процесс обмена сообщениями выполняется между автоматическим устройством и ЭВМ без участия оператора.

Контрольные вопросы

- Назовите классификационные признаки телекоммуникационных каналов связи;
- Классификация проводных телекоммуникационных каналов связи;
- Классификация радио телекоммуникационных каналов связи;
- Классификация каналов по методам разделения канальных сигналов в многоканальных системах связи;
- Классификация телекоммуникационных каналов по способу передачи данных;
- Назовите основные стандарты сотовой связи;
- Назовите классификацию радиочастот и основные частотные диапазоны по международному регламенту радиосвязи;
- Назовите основные диапазоны электромагнитных излучений и их источники;
- Назовите основные стандарты сетей Wi-Fi их базовые параметры;
- Классификация каналов по характеру сигналов на входе и выходе канала.

ГЛАВА 2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ПОКАЗАТЕЛИ И ХАРАКТЕРИСТИКИ КАНАЛОВ СВЯЗИ

Эффективно передаваемая полоса частот. Диапазон частот, в пределах которого амплитудно-частотная характеристика (АЧХ) акустического, радиотехнического, оптического или механического устройства достаточно равномерна для того, чтобы обеспечить передачу сигнала без существенного искажения его формы [2; 10; 11]. Иногда вместо термина «полоса пропускания» используют термин «эффективно передаваемая полоса частот (ЭППЧ)». В ЭППЧ (рис.2) сосредоточена основная энергия сигнала (не менее 90 %). Этот диапазон частот устанавливается для каждого сигнала экспериментально в соответствии с требованиями качества.

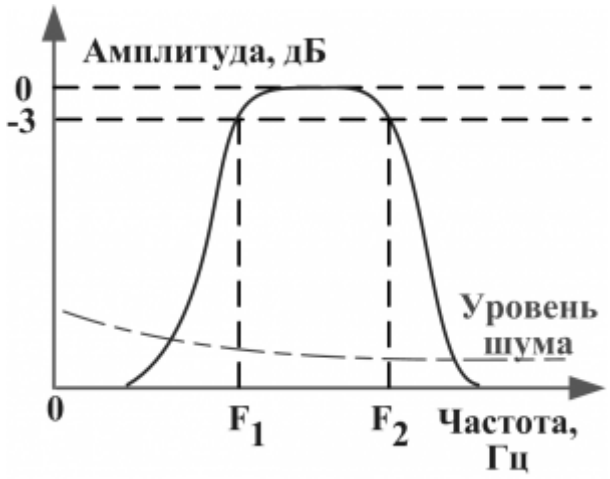


Рис.2. Эффективно передаваемая полоса частот

Термин полоса частот в отношении сигнала связан с понятиями об эффективной ширине спектра сигнала, в которой сосредоточено 90% энергии сигнала (по соглашению), а также о нижней и верхней границах полосы частот сигнала.

Термин полоса частот пропускания употребляется в отношении преобразователей и трактов (интерфейсов) передачи сигналов. Речь идёт об амплитудно-частотной характеристике (АЧХ) этих устройств и о характеристиках полосы пропускания этой АЧХ, которые традиционно измеряются по уровню -3 дБ, как это показано она рисунке выше. За нуль децибел принимается максимальное (или среднее, по соглашению) значение амплитуды сигнала в полосе пропускания. На рисунке частоты F1 и F2 – это нижняя и верхняя частота полосы пропускания соответственно. Нижняя граница F1= 0, если данный преобразователь или тракт пропускает постоянную составляющую сигнала. Чем больше ширина полосы частот пропускания $\Delta F = F2 - F1$ преобразователя или тракта передачи данных, тем выше разрешение (детализация) сигнала по времени, тем выше скорость передачи информации в соответствующем интерфейсе, но в то же время тем больше помех и шумов попадает в полосу пропускания. Если полоса частот сигнала частично или полностью не попадает в полосу частот пропускания преобразователя или тракта, то это приводит к искажению или полному подавлению

сигнала в тракте. С другой стороны, если эффективная полоса частот сигнала многократно уже полосы частот пропускания преобразователя или тракта, то такой случай нельзя считать оптимальным, поскольку в этой физически реализованной системе всегда присутствуют шум и помехи различной природы, которые в общем случае рассредоточены по всей ширине полосы частот пропускания. Области частот пропускания, в которых нет полезных составляющих сигнала, будут добавлять шум, ухудшая соотношение сигнал/шум в данном канале преобразования или передачи сигнала. Исходя из этих посылок, мы вплотную подошли к термину: оптимальная полоса частот пропускания сигнала – это полоса частот пропускания, границы которой согласованы с эффективной полосой частот сигнала.

Неравномерность АЧХ характеризует степень её отклонения от прямой, параллельной оси частот. Неравномерность АЧХ выражается в децибелах. Ослабление неравномерности АЧХ в полосе улучшает воспроизведение формы передаваемого сигнала. Различают: Абсолютную полосу пропускания: $2\Delta\omega = Sa$ и Относительную полосу пропускания: $2\Delta\omega/\omega o = So$

Динамический диапазон. Динамический диапазон — характеристика устройства или системы, предназначенной для преобразования, передачи или хранения некой величины (мощности, силы, напряжения, звукового давления и т. д.), представляющая логарифм отношения максимального и минимального возможных значений величины входного параметра устройства (системы) [2; 10; 11]. Минимальное значение обычно определяется уровнем собственных шумов или внешних помех в устройстве, а максимальное — перегрузочной способностью устройства. Понятие динамический диапазон используется не только в технике, но и в психофизиологии, например, динамический диапазон слышимости человека. В отдельных случаях понятие «динамический диапазон» используется и для выходного параметра (для акустических устройств).

Динамический диапазон радиоприёмника (тракта в целом, функционального узла тракта) — логарифм отношения уровня сигнала на входе радиоприёмника, определенного по одному из критериев, к чувствительности радиоприёмника. По методике определения (по критерию) различают односигнальный динамический диапазон (динамический диапазон по компрессии) и двухсигнальный динамический диапазон (динамический диапазон по блокированию, динамический диапазон по интермодуляции). Динамический диапазон усилителя — логарифм отношения максимальной амплитуды входного сигнала электронного усилителя, при которой искажения сигнала достигают предельно допустимого значения, к чувствительности усилителя [2; 10; 11].

Динамический диапазон канала связи — логарифм отношения максимальной мощности сигналов, пропускаемых каналом, к минимальной $D = 10Lg(\frac{P_{MAX}}{P_{MIN}})$.

Волновое сопротивление. Зависит от типа канала связи. Волновое сопротивление линии передачи зависит от её конструкции и электрофизических параметров применяемых материалов (ε, μ, σ), что совместно определяет погонные параметры линии передачи (ёмкость, индуктивность, сопротивление и проводимость на единицу длины), а также от типа волны, при наличии дисперсии — от частоты электромагнитных колебаний [2; 10; 11].

В длинной линии волновое сопротивление равно (по закону Ома): $Z_0 = (\frac{U_M}{I_M})$ где: U_M — амплитуда напряжения волны (падающей, отраженной или бегущей); I_M — амплитуда силы тока той же волны. В бесконечно длинных линиях нагрузка имеет чисто активный характер, поэтому энергия, запасаемая в индуктивности и ёмкости, одинаковая.

Волновое сопротивление в бесконечно длинных линиях определяется погонными индуктивностью и ёмкостью. Для электромагнитного поля волновое сопротивление среды — отношение амплитуд электрического и магнитного полей электромагнитных волн, распространяющихся в среде. Если волновые сопротивления двух сред, имеющих границу раздела, одинаковы, то на этой границе не происходит отражения электромагнитных волн, даже если диэлектрическая и магнитная проницаемости в средах различны. $Z = (\frac{E_0^-(x)}{H_0^-(x)})$

При распространении электромагнитной волны в среде с диэлектрической ε и магнитной μ проницаемостями амплитудные и мгновенные значения напряжённости электрического *E* и магнитного *H* полей связаны соотношением: $\sqrt{\varepsilon\varepsilon_0}E = .\sqrt{\mu\varepsilon\mu_0}H$ / Отношение *E/H* принято называть волновым сопротивлением среды, поскольку существует формальная аналогия между уравнением $\frac{E}{H} = \sqrt{\frac{\varepsilon\varepsilon_0}{\mu\mu_0}}$ и законом Ома.

Пропускная способность. Метрическая характеристика, показывающая соотношение предельного количества проходящих единиц (информации, предметов, объёма) в единицу времени через канал, систему, узел [2; 10; 11]. Наибольшая возможная в данном канале скорость передачи информации называется его пропускной способностью. Пропускная способность канала есть скорость передачи информации при использовании «наилучших» (оптимальных) для данного канала источника, кодера и декодера, поэтому она характеризует только канал. Номинальная скорость — битовая скорость передачи данных без различия служебных и пользовательских данных. Эффективная скорость — скорость передачи пользовательских данных (нагрузки). Этот параметр зависит от соотношения накладных расходов и полезных данных.

Пропускная способность дискретного (цифрового) канала без помех $C = \log m * V_T$ где m — основание кода сигнала, используемого в канале. Скорость передачи информации в дискретном канале без шумов (идеальном канале) равна его пропускной способности, когда символы в канале независимы, а все m символов алфавита равновероятны (используются одинаково часто). Vт — символьная скорость передачи.

Предельная пропускная способность зависит от ширины полосы пропускания канала, а также от отношения $\frac{P_C}{P_П}$ и определяется по формуле $C_{max} = \Delta F_x \log(1 + \frac{P_C}{P_П})$ двоичных единиц в секунду. Это формула Шеннона, которая справедлива для любой системы связи при наличии флуктуационной помехи.

Помехозащищённость канала связи. Помехозащищенность характеризует способность системы связи противостоять воздействию помех. Помехозащищенность включает в себя такие понятия как скрытность и помехоустойчивость [2; 10; 11]. Помехоустойчивость канала, определяет сопротивления влияние помех которые

создаются во внутренней или внешней среде. Меньше всего помехоустойчивыми есть радиолинии, отличной — оптические линии. Среди всех возможных видов помех исключительное место занимает так называемая флуктуационная помеха типа «белого шума», состоящая из отдельных весьма кратковременных импульсов со случайно изменяющейся амплитудой. «Белый шум» имеет однородный спектр мощности в пределах очень широкой полосы частот. Возникновение объясняется тепловым движением элементарных частиц. Особая роль «белого шума» - он является основным видом помехи, определяющей чувствительность приёмника. Поэтому в теории передачи информации рассматривается воздействие «белого шума».

Способы повышения помехоустойчивости (рис.3): – увеличение избыточности в передаваемом сообщении; – расширение полосы частот; – увеличение соотношения сигнал/шум; – применение помехоустойчивых кодов; - за счет экранирования проводного канала связи; – за счёт фильтрации полезного сигнала.

Скрытность системы связи определяет ее способность противостоять обнаружению и измерению параметров сигнала [2; 10; 11]. Если известно, что в данном диапазоне частот может работать система связи, но параметры ее неизвестны, то в этом случае можно говорить об энергетической скрытности системы связи.

Рис.3. Способы повышения помехоустойчивости каналов связи

Объём сигнала и ёмкость канала. При решении практических задач в теории связи сигнал характеризуют объёмом $V_{\text{С}}$, равным произведению трёх его характеристик: длительности сигнала $\tau_{\text{С}}$, ширины спектра $\Delta F_{\text{С}}$ и превышения средней мощности сигнала над помехой $H_{\text{С}} = \ln\frac{P_C}{P_{\text{П}}}$. В таком случае $V_{\text{С}} = \tau_{\text{С}}\,\Delta F_{\text{С}}\,H_{\text{С}}$. Если эти характеристики разложить параллельно осям декартовой системы, то получится объём параллелепипеда, поэтому такое произведение называется объёмом сигнала [8; 10; 11]. Длительность сигнала определяет интервал времени его существования. Ширина

спектра сигнала – это интервал частот, в котором размещается ограниченный спектр частот сигнала, т.е. $\Delta F_{\text{С}} = \frac{1}{\tau_C}$.

Канал связи по своей физической природе в состоянии пропустить эффективно лишь сигналы, спектр которых лежит в ограниченной полосе частот ΔF_k при допустимом диапазоне изменения мощности H_k. Кроме того, канал связи предоставляется отправителю сообщения на вполне определённое время τ_K.

Следовательно, по аналогии с сигналом в теории связи введено понятие ёмкости канала V_k, которая определяется: $V_k = \tau_k \, \Delta F_k \, H_k$; $\Delta F_k \approx \frac{1}{\tau_k}$. Необходимым условием передачи сигнала с объёмом $V_{\text{С}}$ по каналу связи, ёмкость которого равна V_k, есть $V_k > V_{\text{С}}$ или. Физические характеристики сигнала могут быть изменены, но при этом уменьшение одной из них сопровождается увеличением другой.

Достоверность передачи данных (для цифровых каналов)- вероятность искажения бита из-за воздействия помех и наличия шумов в канале связи (обычно для канала связи без дополнительных средств защиты составляет от 10~4 до 10~6) [8;11]; иногда используется единица измерения BER (Bit Error Rate) - интенсивность битовых ошибок.

Секретность и имитостойкость канала связи. Обеспечение секретности - лишение противника возможности извлечь информацию из канала связи. Имитостойкость - лишение противника возможности ввести ложную информацию в канал связи или изменить сообщение так, чтобы изменился его смысл [8; 10; 11]. В случае проводной связи главной является проблема имитостойкости, поскольку вызванная сторона не может часто определить, от кого сообщение. Подслушивание, требующее подключения к проводам, технически более сложно и юридически более опасно. В случае радиосвязи ситуация прямо противоположная. Перехват здесь является пассивным и сопряжен с незначительной юридической опасностью, тогда как введение информации связано с риском обнаружения незаконного передатчика и юридического преследования.

Затухание (ослабление) сигнала. Затухание показывает, как сильно уменьшается мощность эталонного синусоидального сигнала на выходе канала связи по отношению к мощности сигнала на входе этого канала. Затухание обычно измеряется в децибелах (дБ) и вычисляется по следующей формуле: В = 10Log10Рвых/ Рвх = 20Log10Uвых/ Uвх , где Рвых - мощность сигнала на выходе канала, Рвх - мощность сигнала на входе канала [8; 10; 11]. Затухание всегда рассчитывается для определенной частоты и соотносится с длиной канала. На практике всегда пользуются понятием "погонное затухание", т.е. затухание сигнала на единицу длины канала, например, затухание 0,1дБ/метр.

Помехи и шумы в каналах связи. Помеха — всякое постороннее воздействие на полезный сигнал, оказывающее мешающее действие при его приеме и проявляющее себя изменением его формы. Классификация помех [8; 10; 11] приведена на рис.4.

Аддитивной является сумма полезного сигнала Sм(t) и помехи N0(t): Z(t)=Sм(t)+N0(t)

Мультипликативной является произведение полезного сигнала и помехи: Z(t)=Sм(t)xN0(t)

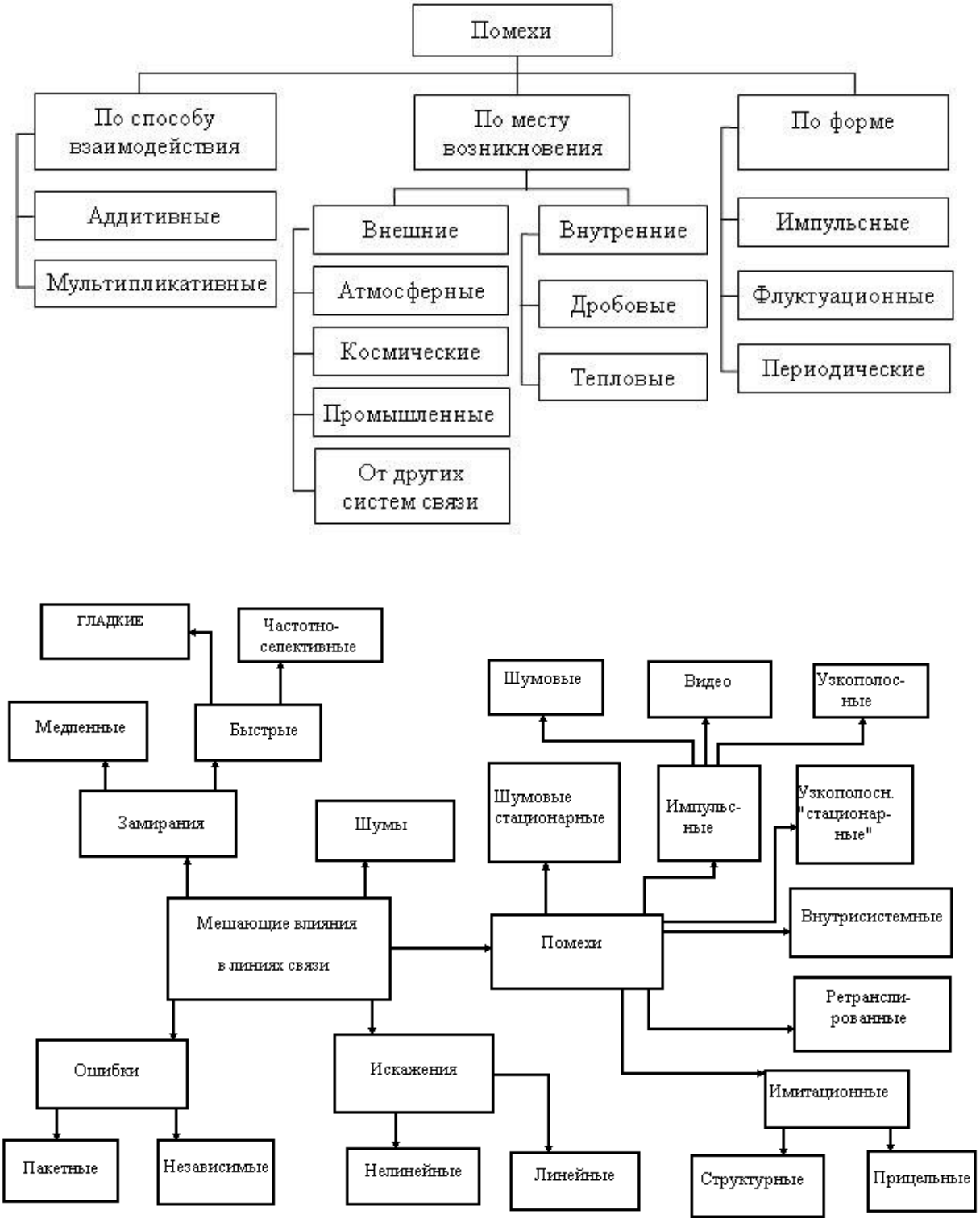


Рис.4. Классификация помех и мешающих влияний в линиях связи

Внешними являются помехи, возникающие вне канала, к ним относятся:

- атмосферные возникают в атмосфере земли и могут быть вызваны грозовыми разрядами, осадками, пылевыми бурями, северным сиянием;

- космические возникают в космическом пространстве и могут быть вызваны солнечной активностью, космическими телами;

- промышленные могут быть вызваны промышленными установками: высокочастотными генераторами, высоковольтными линиями электропередачи, электрифицированным транспортом;

- от других систем связи обуславливаются воздействием на полезный сигнал одной системы связи сигналов других систем, например, прослушивание радиопередач или другого разговора в телефонной трубке, прием на одной частоте срезу нескольких радиопередач.

Внутренними являются помехи, возникающие внутри канала, к ним относятся собственные шумы, которые, в свою очередь, подразделяются на:

- тепловые — обусловлены хаотическим движением электрических зарядов в проводниках;

- дробовые — обусловлены неоднородной плотностью носителей заряда в проводниках.

Собственные шумы не могут быть устранены, т. к. они вызваны физикой процесса передачи электрической энергии.

Импульсными помехами являются сконцентрированные по времени скачки тока или напряжения. Флуктуационные помехи вызваны флуктуациями (отклонением от среднего значения) тока и напряжения. Периодические помехами являются периодические скачки тока или напряжения. Различают нелинейные и линейные искажения.

Нелинейными являются искажения, при которых в спектре сигнала появляются новые составляющие. Такие искажения вызваны нелинейностью характеристик элементов и блоков, входящих в аппаратуру системы связи. Линейными являются искажения, при которых в спектре сигнала не появляются новые составляющие. Такие искажения возникают из–за изменения соотношения между составляющими спектра сигнала. Линейные искажения бывают амплитудно-частотными (АЧИ), при которых изменяются амплитуды составляющих спектра сигнала и фазо-частотные (ФЧИ), при которых изменяются фазы составляющих спектра.

Замирания. Случайные изменения параметров амплитуды сигнала и времени запаздывания сигнала приводят к непрерывному изменению уровня принимаемого сигнала, которое называется замираниями или федингами [8; 10; 11]. Замирания обусловлены интерференцией в точке приема многих лучей, прошедших различные пути в результате многократного отражения радиоволн от различных слоев атмосферы. Нерегулярный характер изменения высоты и толщины этих слоев, а также их

электронной концентрации приводит к случайным изменениям амплитуд и фаз отдельных лучей на входе приемника. В итоге, результирующий сигнал подвержен замираниям по случайному закону.

Кроме интерференционных замираний наблюдаются поляризационные замирания, обусловленные вращением плоскости поляризации волны под действием магнитного поля Земли. В зависимости от ширины спектра сигнала и свойств среды распространения различают гладкие и селективные замирания. В свою очередь замирания могут быть медленными и быстрыми. Когда взаимное запаздывание приходящих лучей соизмеримо с длительностью элемента сигнала, явление многолучевого распространения вызывает не только замирания сигнала, но и наложение соседних элементов сигнала друг на друга. Это явление называется радиоэхо, а запаздывающий луч - эхосигналом. Медленные изменения амплитуды сигнала, приводящие к медленным замираниям, вызываются суточными и сезонными изменениями состояния тропосферы и ионосферы. Быстрые замирания обусловлены, главным образом, многолучевым распространением радиоволн. Типичными представителями каналов с переменными параметрами являются коротковолновые каналы радиосвязи, а также УКВ-каналы тропосферной, ионосферной и метеорной радиосвязи.

Контрольные вопросы

- Что такое амплитудно-частотная характеристика (АЧХ) и неравномерность АЧХ канала связи;
- Что такое динамический диапазон канала связи;
- Пропускная способность канала связи;
- Затухание сигналов и волновое сопротивление линии передачи в каналах связи;
- Понятие секретности и имитостойкости канала связи;
- Понятие помехозащищённости канало связи и методы повышения помехозащищенности каналов связи;
- Классификация помех и шумов в каналах связи;
- Понятие аддитивной и мультипликативной помехи в каналах связи;
- Понятие нелинейных искажений в каналах связи;
- Замирания сигналов в каналах связи.

ГЛАВА 3. ОСНОВНЫЕ ПОКАЗАТЕЛИ И ХАРАКТЕРИСТИКИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

3.1. Общая классификация технических каналов утечки информации

Технические каналы утечки информации (ТКУИ) классифицируются по различным признакам [4;12-15], в том числе:

каналы утечки информации, обрабатываемой техническими средствами обработки информации (ТСОИ)*, делятся на:*

-электромагнитные, которые в сою очередь можно разделить на:

- перехват ПЭМИ (побочные электро-магнитные излучения) элементов ТСОИ;
- перехват ПЭМИ на частотах работы ВЧ-генераторов в ТСОИ и ВТСС (вторичные технические средства и системы);
- перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты ТСОИ;

-электрические:

- съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников;
- съем информативных сигналов с линий электропитания ТСОИ;
- съем информативных сигналов с цепи заземления ТСОИ и ВТСС;
- съем информации путем установки в ТСОИ электронных устройств перехвата информации, комплексированных с устройствами передачи информации по радиоканалам;

-параметрические:

- перехват информации путем ВЧ-облучения ТСОИ.

Каналы утечки акустической (речевой) информации делятся на

- воздушные:

- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по сети электропитания;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по телефонным линиям;
- перехват акустических сигналов микрофонами, комплексированными с устройствами их подключения к телефонным линиям по сигналу вызова от внешнего телефонного абонента;
- перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям.

- акустоэлектрические:

- перехват акустических колебаний через ВТСС, обладающие микрофонным эффектом, путем подключения их к соединительным линиям;
- перехват акустических колебаний через ВТСС, путем ВЧ-навязывания,

-вибрационные:

- перехват акустических сигналов с помощью электронных стетоскопов;
- перехват акустических сигналов стетоскопами, комплексированными с устройствами перехвата информации по радиоканалу, оптическому каналу в ИК-диапазоне, по трубам водоснабжения, отопления, металлоконструкциям и т.д.

-параметрические:

- перехват акустического сигнала путем приема и детектирования ПЭМИ (на частотах ВЧ-генераторов) ТСОИ и ВТСС при модуляции информативным сигналом;
- перехват акустического сигнала путем ВЧ-облучения специальных полуактивных закладных устройств.

- оптикоэлекторонный (лазерный):

- перехват акустического сигнала путем лазерного зондирования оконных стекол.

Съем информации, передаваемой по каналам связи может производиться по:

***- электромагнитному каналу*:**

-при перехвате информации, передаваемой по каналам радио- и радиорелейной связи;

-при перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи.

- ТКУИ, передаваемой по кабельным линиям связи:

- электрическому – при съеме информации путем контактного подключения к кабельным линиям связи;
- индукционному – при бесконтактном съеме информации с кабельных линий связи.

Каналы скрытого видеонаблюдения и съемки делятся на каналы:

- наблюдения за объектом (съем видовой информации):

- днем: наблюдение за объектами с использованием оптических приборов (монокуляторов, подзорных труб, биноклей, телескопов);
- наблюдение за объектами с использованием телевизионных систем, в т.ч. с устройствами передачи изображения по радиоканалу;

- ночью: наблюдение за объектами с использованием приборов ночного видения;
- наблюдение за объектами с использованием телевизионных систем, в т.ч. комплексированных с приборами ночного видения;
- наблюдение за объектами с использованием телевизионных систем.

- съемки объектов:

- днем: съемка объектов с использованием фотоаппаратов;
- съемка объектов с использованием телевизионных систем, комплексированных с портативными устройствами видеозаписи (передачи изображения по радиоканалу).

- ночью: съемка объектов с использованием фотоаппаратов, комплексированных с прибором ночного видения;

- съемка объектов с использованием телевизионных систем, в т.ч. комплексированных с прибором ночного видения и портативными устройствами видеозаписи (передачи изображения по радиоканалу);
- съемка объектов с использованием систем, комплексированных с портативными устройствами видеозаписи.

- ***съемки (снятии копии) документов:*** съемка документов с использованием портативных фотоаппаратов.

3.2. Общая классификация технических средств защиты информации от утечки по техническим каналам

Общая классификация технических средств защиты информации [4;14;15] представлена на рис.5. Классификация программных средств защиты информации [16;17;18] представлена на рис.6.

Рис.5. Общая классификация технических средств защиты информации

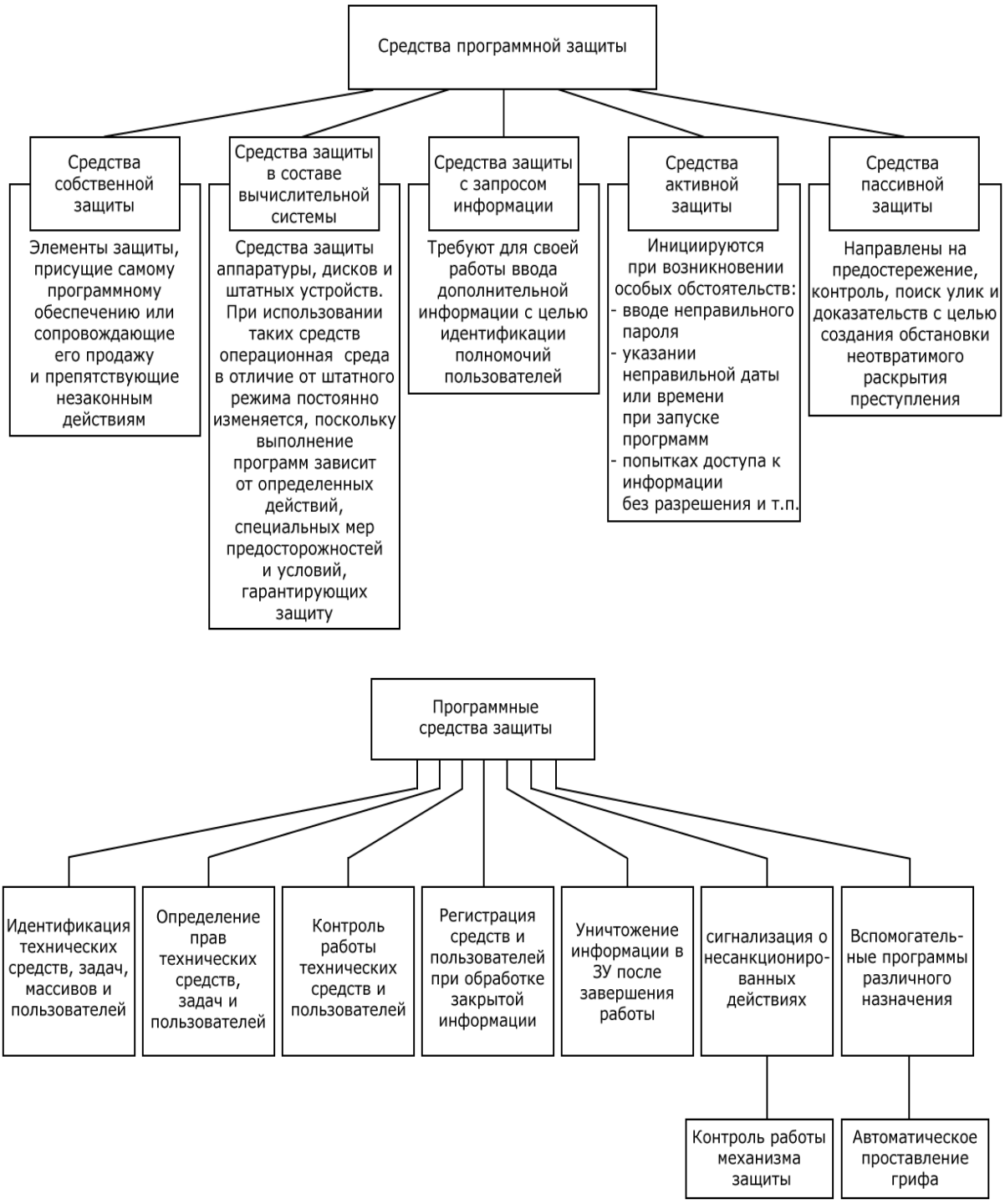


Рис.6. Классификация программных средств защиты информации

3.3. Основные термины, определения и технические характеристики средств защиты информации от утечки акустической информации

Характеристики акустического канала. Источники акустических колебаний разделяют на: - первичные – механические колебательные системы, например, органы речи человека, музыкальные инструменты, струны, звуки работающей техники; - вторичные – электроакустические преобразователи – устройства для преобразования акустических колебаний в электрические и обратно (пьезоэлементы, микрофоны, телефоны, громкоговорители и др.) и технические устройства в которых эти преобразователи используются. Органы слуха человека способны воспринимать колебания частотой от 16-20 Гц до 16-20 кГц. Колебания с указанными частотами называют звуковыми. Неслышимый звук с частотой ниже 16 Гц называют инфразвуком, выше 20 кГц – (в пределах $1{,}5*10^4 – 10^9$ Гц) – ультразвуком, в пределах $10^9 – 10^{13}$ Гц – гиперзвуком. Среди слышимых звуков следует также особо выделить фонетические, речевые звуки и фонемы (из которых состоит устная речь) и музыкальные звуки (из которых состоит музыка).

Звуковые колебания характеризуются звуковым давлением, интенсивностью звука, громкостью, мощностью звука [19;20;21;4;22]. Одной из характеристик любой произвольной точки звукового поля является звуковое давление, вызываемое переменной составляющей звуковой волны. Весь частотный диапазон звука можно разделить на части (таблица 6.).

Таблица 6

Частотный диапазон звука

Тип звука	*Частота, Гц*
низкочастотный звук	16 – 400
среднечастотный звук	400 – 1 000
высокочастотный звук	1 000 – 20 000
Шум	16 – 44
Речь Музыка	44 – 2 300
Свист	2 300 – 20 000

Кроме того, интервал музыкальных частот делят на октавы. Октава – это интервал частот, заключённый между двумя граничными значениями, верхняя из которых вдвое больше нижней (таблица 7)

Таблица 7

Общепринятые октавные полосы частот

Октавные полосы частот	ν_{min}, *Гц*	ν_{max}, *Гц*	$\nu_{ср}$, *Гц*
1	45	90	63
2	90	180	125
3	180	355	250
4	355	710	500
5	710	1400	1000
6	1400	2800	2000
7	2800	5600	4000
8	5600	12000	8000

Звуковое давление – это переменная часть давления, возникающего при прохождении звуковой волны в среде распространения. Измеряется эта сила, действующая на единицу площади в паскалях (Па).

Звуковое давление в воздухе изменяется от 10^{-5} Па вблизи порога слышимости до ~ 10^3 Па – болевой порог при самых громких звуках (шум реактивного самолета). При средней громкости разговора переменная составляющая звукового давления порядка 0,1 Па.

Минимальное звуковое давление, на которое реагирует человеческое ухо, составляет $2*10^{-5}$ Па, максимально же воспринимаемое без ощущения боли звуковое давление 10^2 Па. Следовательно, диапазон звуковых давлений, воспринимаемых человеческим ухом, составляет 10^7. Для характеристики звука часто применяется уровень звукового давления, выраженного в децибелах (дБ) – отношение величины данного звукового давления Р к пороговому значению звукового давления равному $P_{ПОР} = 2*10^{-5}$ Па. $N = 20 \lg\left(\frac{P}{P_{ПОР}}\right)$ дБ.

Плоскость между порогом слышимости и болевым порогом называют плоскостью слышимости [19;20;21;4;22]. Эта плоскость характеризуется следующими данными: по частоте колебаний – 20Гц – 20 кГц; по звуковому давлению – 0 – 140 дБ.

Область разговорной речи на рис.7 обозначена горизонтальной штриховкой (по частоте колебаний 0,2 – 4,0 кГц, по звуковому давлению 35 – 85 дБ), негромкой музыки– вертикальной штриховкой.

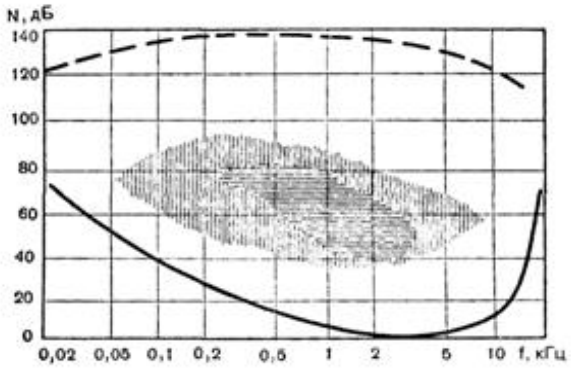


Рис.7. Плоскость слышимости человеческого уха

Энергетической характеристикой звуковых колебаний является **интенсивность звука**, которая зависит от амплитуды звукового давления, а также от свойств среды распространения и формы волны. Интенсивность – это среднее по времени значение мощности звука, отнесенное к единице площади. Интенсивность звука оценивается уровнем интенсивности по шкале децибел:

$N = 10 \lg\left(\frac{J}{J_o}\right)$, где J – интенсивность данного звука, $J_o = 10^{12}$ Вт/м^2.

С интенсивностью звука связана **громкость звука** – величина, характеризующая слуховое ощущение от данного звука. Громкость звука сложным образом зависит от звукового давления (интенсивности звука). При неизменной частоте и форме колебаний громкость звука растет с увеличением интенсивности звука (звукового

давления). При одинаковом звуковом давлении громкость звука гармонических колебаний различной частоты различна, т.е. на разных частотах одинаковую громкость могут иметь звуки разной интенсивности. Громкость звука — субъективное восприятие силы звука (абсолютная величина слухового ощущения). Также на громкость звука влияют его спектральный состав, локализация в пространстве, тембр, длительность воздействия звуковых колебаний, индивидуальная чувствительность слухового анализатора человека и другие факторы [19;20;21;4;22].

Различают продольные и поперечные звуковые волны в зависимости от соотношения направления распространения волны и направления механических колебаний частиц среды распространения. Звуковые волны могут служить примером колебательного процесса. Всякое колебание связано с нарушением равновесного состояния системы и выражается в отклонении её характеристик от равновесных значений с последующим возвращением к исходному значению. Для звуковых колебаний такой характеристикой является давление в точке среды, а её отклонение— звуковым давлением.

Мгновенное значение звукового давления в точке среды изменяется как со временем, так и при переходе к другим точкам среды, поэтому практический интерес представляет среднеквадратичное значение данной величины, связанное с интенсивностью звука:

$I = \frac{<\rho^2>_t}{Z_S}$ где I— интенсивность звука, ρ— звуковое давление, Z_S — удельное акустическое сопротивление среды, $<>_t$— усреднение по времени. При рассмотрении периодических колебаний иногда используют амплитуду звукового давления; так, для синусоидальной волны $\rho = \rho_o sin(\varpi t + \varphi)$; $< \rho^2 >_t = \frac{\pi \rho_0}{\varpi}$; $I = \frac{\pi \rho^2{}_0}{\varpi Z_S}$ где ρ_0 — амплитуда звукового давления.

Уровень звукового давления (англ. *SPL, Sound Pressure Level*)— измеренное по относительной шкале значение звукового давления, отнесённое к опорному давлению ρ_{SPL} = 20 мкПа, соответствующему порогу слышимости синусоидальной звуковой волны частотой 1 кГц: $SPL = 20lg\frac{p}{20\ \mu\text{Па}}$ дБ.

Уровни звукового давления от различных источников [19;20;21;4;22]**:**

- 0 дБ SPL — специальная измерительная камера;
- 5 дБ SPL — почти ничего не слышно;
- 10 дБ SPL — почти не слышно — шёпот, тиканье часов, тихий шелест листьев;
- 15 дБ SPL — едва слышно — шелест листьев;
- 20 дБ SPL — едва слышно — уровень естественного фона на открытой местности при отсутствии ветра, норма шума в жилых помещениях;
- 25 дБ SPL — тихо — сельская местность вдали от дорог;
- 30 дБ SPL — тихо — настенные часы;
- 35 дБ SPL — хорошо слышно — приглушённый разговор;
- 40 дБ SPL — хорошо слышно — тихий разговор, учреждение (офис) без источников шума, уровень звукового фона днём в городском помещении с закрытыми окнами выходящими во двор;
- 50 дБ SPL — отчётливо слышно — разговор средней громкости, тихая улица, стиральная машина;

- 60 дБ SPL — шумно — обычный разговор, норма для контор;
- 65 дБ SPL — шумно — громкий разговор на расстоянии 1 м;
- 70 дБ SPL — шумно — громкие разговоры на расстоянии 1 м, шум пишущей машинки, шумная улица, пылесос на расстоянии 3 м;
- 75 дБ SPL — шумно — крик, смех с расстояния 1м; шум в железнодорожном вагоне;
- 80 дБ SPL — очень шумно — громкий будильник на расстоянии 1 м; крик; мотоцикл с глушителем; шум работающего двигателя грузового автомобиля;
- 85 дБ SPL — очень шумно — громкий крик, мотоцикл с глушителем;
- 90 дБ SPL — очень шумно — громкие крики, пневматический отбойный молоток, тяжёлый дизельнй грузовик на расстоянии 7 м, грузовой вагон на расстоянии 7 м;
- 95 дБ SPL — очень шумно — вагон метро на расстоянии 7 м;
- 100 дБ SPL — крайне шумно — громкий автомобильный сигнал на расстоянии 5—7 м, кузнечный цех, очень шумный завод;
- 110 дБ SPL — крайне шумно — шум работающего трактора на расстоянии 1 м, громкая музыка, вертолёт;
- 115 дБ SPL — крайне шумно — пескоструйный аппарат на расстоянии 1 м;
- 120 дБ SPL — почти невыносимо — болевой порог, гром (иногда до 120 дБ), отбойный молоток, на расстоянии 1 м;
- 130 дБ SPL — боль — сирена, шум клёпки котлов;
- 140 дБ SPL — травма внутреннего уха — взлёт реактивного самолёта на расстоянии 25м, максимальная громкость на рок-концерте;
- 150 дБ SPL — контузия, травмы — взлёт ракеты;
- 160 дБ SPL — шок, травмы, возможен разрыв барабанной перепонки — выстрел из ружья близко от уха; ударная волна от сверхзвукового самолёта или взрыва давлением 0,002 МПа;
- 170 дБ SPL — воздушная ударная волна давлением 0,0063 МПа;
- 180 дБ SPL — воздушная ударная волна давлением 0,02 МПа, длительный звук с таким давлением вызывает смерть;
- 190 дБ SPL — воздушная ударная волна давлением 0,063 МПа;
- 194 дБ SPL — воздушная ударная волна давлением 0,1 МПа, равным атмосферному давлению, возможен разрыв лёгких;
- 200 дБ SPL — воздушная ударная волна давлением 0,2 МПа, возможна смерть.

Если произвести резкое смещение частиц упругой среды в одном месте, например, с помощью поршня, то в этом месте увеличится давление. Благодаря упругим связям частиц давление передаётся на соседние частицы, которые, в свою очередь, воздействуют на следующие, и область повышенного давления как бы перемещается в упругой среде. За областью повышенного давления следует область пониженного давления, и, таким образом, образуется ряд чередующихся областей сжатия и разрежения, распространяющихся в среде в виде волны. Каждая частица упругой среды в этом случае будет совершать колебательные движения.

В жидких и газообразных средах, где отсутствуют значительные колебания плотности, акустические волны имеют продольный характер, то есть направление колебания частиц совпадает с направлением перемещения волны. В твёрдых телах,

помимо продольных деформаций, возникают также упругие деформации сдвига, обусловливающие возбуждение поперечных (сдвиговых) волн; в этом случае частицы совершают колебания перпендикулярно направлению распространения волны. Скорость распространения продольных волн значительно больше скорости распространения сдвиговых волн.

Колебательная скорость звука измеряется в м/с или см/с. В энергетическом отношении реальные колебательные системы характеризуются изменением энергии вследствие частичной её затраты на работу против сил трения и излучение в окружающее пространство. В упругой среде колебания постепенно затухают.

Для характеристики затухающих колебаний используются коэффициент затухания (S), логарифмический декремент (D) и добротность (Q) [19;20;21;4;22].

Коэффициент затухания отражает быстроту убывания амплитуды с течением времени. Если обозначить время, в течение которого амплитуда уменьшается в e = 2,718 раза, через τ, то: $S = 1/\tau$.

Уменьшение амплитуды за один цикл характеризуется логарифмическим декрементом. Логарифмический декремент равен отношению периода колебаний ко времени затухания $D = T/\tau$.

Свойство среды проводить акустическую энергию, в том числе и ультразвуковую, характеризуется акустическим сопротивлением. *Акустическое сопротивление* среды выражается отношением звуковой плотности к объёмной скорости ультразвуковых волн. Удельное акустическое сопротивление среды устанавливается соотношением амплитуды звукового давления в среде к амплитуде колебательной скорости её частиц. Чем больше акустическое сопротивление, тем выше степень сжатия и разрежения среды при данной амплитуде колебания частиц среды. Численно, удельное акустическое сопротивление среды (Z) находится как произведение плотности среды ρ на скорость (с) распространения в ней ультразвуковых волн $Z = \rho c$. Удельное акустическое сопротивление измеряется в паскаль-секунда на метр (Па·с/м) или дин•с/см³ (СГС); 1 Па·с/м = 10^{-1} дин • с/см³. Акустическое сопротивление среды определяется поглощением, преломлением и отражением ультразвуковых волн.

Звуковое или *акустическое давление* в среде представляет собой разность между мгновенным значением давления в данной точке среды при наличии звуковых колебаний и статического давления в той же точке при их отсутствии. Иными словами, звуковое давление есть переменное давление в среде, обусловленное акустическими колебаниями. Максимальное значение переменного акустического давления (амплитуда давления) может быть рассчитано через амплитуду колебания частиц: $P = 2\pi f \rho c A$ где P— максимальное акустическое давление (амплитуда давления); f — частота; с— скорость распространения звука; ρ — плотность среды; A — амплитуда колебания частиц среды.

На расстоянии в половину длины волны (λ/2) амплитудное значение давления из положительного становится отрицательным, то есть разница давлений в двух точках, отстоящих друг от друга на λ/2 пути распространения волны, равна 2P.

Скорость звука — скорость распространения звуковых волн в среде. Как правило, в газах скорость звука меньше, чем в жидкостях, а в жидкостях скорость звука меньше, чем в твёрдых телах, что связано в основном с убыванием сжимаемости веществ в этих фазовых состояниях соответственно. В среднем, в идеальных условиях,

в воздухе скорость звука составляет 340—344 м/с. Скорость звука в любой среде вычисляется по формуле: $c = \sqrt{\frac{1}{\beta\rho}}$ где β — адиабатическая сжимаемость среды; ρ— плотность.

Характеристики речи. Речь представляет собой колебания сложной формы, зависящей от произносимых слов, тембра голоса, интонации, пола и возраста говорящего. Основными параметрами, используемыми при описании речевого сигнала, являются: статистическое распределение звуков, слогов и слов при произношении речи; временные характеристики звуков; основной тон речи; спектр речи; распределение формантных частот [19;20;21;4;22].

Согласные звуки также разделяют на несколько подгрупп — твердые, мягкие и др. Гласные звуки составляют примерно 43,5 %, а согласные — 56,5 % общего числа звуков, при этом невокализованные звуки составляют 32 %. Наиболее распространенный гласный звук — это *а*, самый распространенный согласный звук —*г*. Среди гласных звуков наиболее редким является звук *э,* среди согласных —*фь*. Согласные фонемы (звуки) по типу делят на *звонки* и *глухие*, а по способу образования – на *щелевые* (звонкие - *в, з, ж* и глухие –*ф, с, ш, х,*), *взрывные*, т.е. *смычные* (звонкие - *б, г, д* и глухие - *п, т, к,*), *сонаты* (носовые - *м, н*, щелевые -*л, й*, дрожащие - *р*) и *аффрикаты* (*ц, ч*). Каждый звук является реализацией случайного процесса с определенными характеристиками. Длительность отдельных звуков речи составляет 20...350 мс. При этом гласные звуки имеют бо́льшую длительность (в среднем около 200 мс), чем согласные (около 80 мс, а звук "п" - около 30 мс). Звонкие звуки речи, особенно гласные, имеют высокий уровень интенсивности, глухие - низкий - в среднем на 20 дБ ниже уровня гласных. Динамический диапазон уровней речи находится в пределах 35...45 дБ. Речь с физической точки зрения состоит из последовательности звуков речи с паузами между их группами. Паузой считается отсутствие речи в течение времени, большего 350 мс. В целом средняя длительность пауз составляет приблизительно 16 % длительности речи, а средняя скорость речи 10... 15 звуков/с. Темп речи может изменяться в широких пределах, длительность фонем, слогов и пауз также изменяется, причем длительность гласных звуков изменяется в большей степени.

Важной характеристикой вокализованных звуков [19;20;21;4;22] является *частота основного тона* (ОТ) $F_{О.Т.}$ - частота колебаний голосовых связок или частота первой гармоники спектра вокализованных звуков; $T_0 = 1 / F_{О.Т.}$- период основного тона голоса. У вокализованных звуков спектр является дискретным с большим числом (до 40) гармоник, которые имеют частоту, кратную частоте основного тона. Частота ОТ изменяется в пределах от 60...70 Гц для низких мужских голосов до 450...500 Гц для высоких женских голосов. Средняя частота ОТ для мужских голосов 130... 150 Гц, для женских — 250 Гц. Медленное изменение частоты основного тона при произнесении речи создает эмоциональную окраску и называется *интонацией*. У каждого человека свой диапазон изменения основного тона (немного более октавы) и своя интонация, играющая большую роль в процессе узнавания говорящего. Пример плотности распределения вероятности частоты ОТ [19;20;21;4;22], представлен на рис.8.

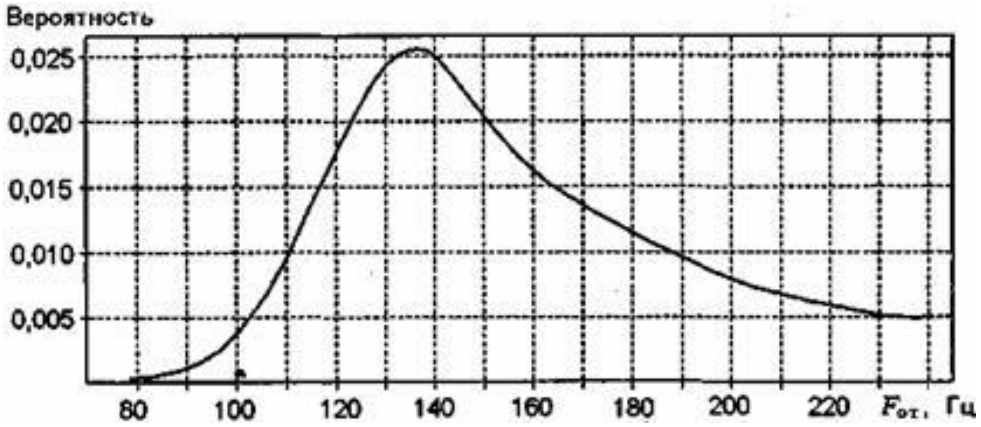


Рис.8. Плотность распределения вероятности частоты основного тона (получено в течение 15 мин для речи 15 мужчин – дикторов в возрасте около 20 лет)

Спектр речи — зависимость среднего в течение длительного времени наблюдения спектрального уровня речи от частоты $B_p(f)$ - весьма широк (примерно от 50 до 10000 Гц). Спектр русской речи, усредненный для мужских и женских голосов [19;20;21;4;22], представлен на рис.9. Как отсюда следует, основная энергия в спектре речи сосредоточена в области низких частот. Максимальный уровень спектральной плотности речи лежит вблизи частоты 300 Гц, а наиболее «мощные» спектральные составляющие человеческого голоса сосредоточены в узкой полосе 200...600 Гц. Каждому звуку речи соответствует свое распределение энергии по частотному диапазону, называемое *формантным рисунком.* Формантные частоты, на которых происходит максимальное увеличение амплитуды спектральных составляющих, образуют *формантные области* частотного диапазона.

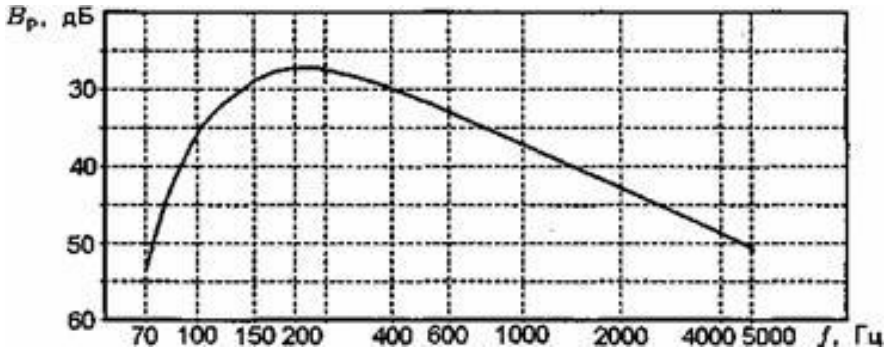


Рис.9. Спектр русской речи

Спектральный состав звуков речи различен. Например, для гласных и звонких согласных (вокализованных звуков речи) энергетический спектр (формантный рисунок) [19;20;21;4;22] имеет вид, представленный на рис.10. Звонкие звуки имеют ярко выраженный дискретный спектр. Это объясняется природой образования гласных звуков, а дискретность определяется частотой основного тона: чем меньше частота ОТ, тем чаще будет заполнение спектра звука.

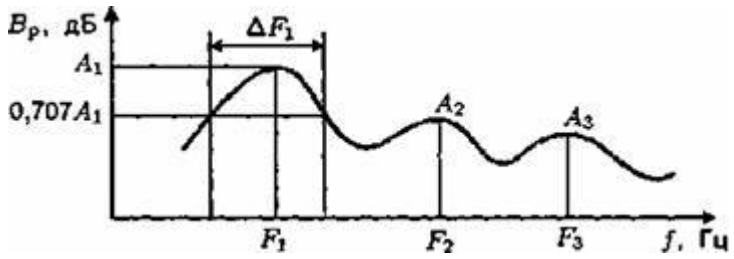


Рис.10. Формантный рисунок вокализованных звуков: A_1-A_3 - амплитуды формант; F_1-F_3 - частоты формант; DF_1 - ширина первой форманты

Форманта характеризуется амплитудой A_i, частотой F_i, и шириной полосы DF_i. Различные звуки имеют разное число формант: гласные - до четырех формант, глухие согласные до 5-6 формант. Наиболее информативны первые три форманты: F_1, F_2 и F_3. Наиболее вероятные частоты расположения: первой форманты F_1 –150 – 900 Гц; второй форманты F_2 – 550 – 2800 Гц; третьей форманты F_3 – 1500 – 3400 Гц. Первые две (*основные*) форманты определяют произносимый звук речи, а остальные (*вспомогательные*) характеризуют индивидуальную для каждого человека окраску, тембр речи. Формантный рисунок глухих звуков выражен слабо. У них спектр не дискретный, а сплошной и характеризуется только огибающей спектра. Так, для звука "С" максимум спектральной плотности лежит вблизи частот 5000 – 8000 Гц. В полосе частот 1500 – 8000 Гц находится спектр согласных звуков и, в частности, фрикативных согласных ("в", "ф", "з", "с", "ж", "ш", "х", "щ"). Восприятие их особенно важно для разборчивости речи.

Реверберация. За счет многократных переотражений акустической волны в замкнутой среде распространения возникает явление послезвучания - реверберация. Величина реверберации оценивается временем T_p после выключения источника звука, в течение которого энергия звука уменьшается на 60дБ. Вследствие многократных переотражений на мембрану микрофона в помещении оказывают давление акустические волны, распространяющиеся разными путями от источника звука. Чем больше размеры помещения и меньше коэффициент поглощения ограждающих поверхностей, тем больше время реверберации. При большом времени реверберации помещение кажется гулким. Время реверберации менее 0,85 с незаметно для слуха. Для большинства помещений организаций их объемы и акустическая отделка время реверберации мало (0,2-0,6) с и его можно не учитывать при оценке разборчивости [23;26]. Для концертных залов, имеющих существенно большие размеры, время реверберации определяет их акустику. Установлено, что в малых помещениях объемом V до 350м^2 оптимальной является реверберация со временем до 1,06 сек. При увеличении объема помещения время реверберации пропорционально повышается и принимает для V=27000 м^3 значение около 2 сек. Время реверберации в помещении объемом V вычисляется по формуле Эйринга : $T_P \approx -\frac{0.07V}{S\ln(1-\alpha_{\text{СР}})}$, где S - суммарная площадь всех поверхностей помещения; $\alpha_{\text{СР}} = \sum_{k=1}^{K} \alpha_k S_k$ - средний коэффициент звукопоглощения в помещении; $S_к$ и $\alpha_к$ - площади и коэффициенты поглощения ограждающих поверхностей соответственно. При распространении звука в конструкциях зданий, особенно, в трубопроводах возникают реверберационные

искажения, снижающие разборчивость речи на 15-20%. Ухудшение разборчивости речи при прохождении звука через различные строительные конструкции иллюстрируются данными в таблице 8 [19;20;21;4;22].

Таблица 8.

Ухудшение разборчивости речи при прохождении звука через различные строительные конструкции

Тип конструкции	Ожидаемая разборчивость слогов, %
Кирпичная стена (1 кирпич)	25/0
Гипсолитовая стена	90/0
Деревянная стена	99/63
Дверь обычная филенчатая	100/73
Дверь двойная	95/36
Окно с одним стеклом 3 мм	90/33
Окно с одним стеклом 6 мм	87/15
Оконный блок 2х3 мм	82/0
Вентиляционный канал 20 м	90/2
Бетонная стена	88/0
Перегородка внутренняя	96/80
Трубопровод (в соседнем помещении)	95/55
Трубопровод (через этаж)	87/36

Примечание: в числителе указаны значения разборчивости речи при малом уровне акустических шумов, в знаменателе - при сильном.

Звукоизоляция помещений. Затухание акустической волны на границе контролируемой зоны зависит от множества факторов, таких как конструкция помещения, материал стен, тип и количество дверей и окон, наличие звукопоглощающих элементов и т.п. Расчет распространения акустических волн с объекта защиты проводится от уровня сигнала 80 дБ [23;21;4;22]. Учитывая, что средняя громкость звука говорящего в служебном помещении составляет около 50 ...60 дБ, то в зависимости от категории помещения его звукоизоляция должна быть не менее норм, приведенных в таблице 9 [23;21;4;22;15]. Затухание акустической волны на различных строительных конструкциях представлены в таблицах 9; 10; 11; 12; 13 [22].

Таблица 9

Требования к звукоизоляции помещений

Частота, Гц	**Категория выделенного помещения, дБ**		
	1	2	3
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных отделочных материалов. Двери имеют меньшие по сравнению со стенами и перекрытиями зазоры и щели.

Таблица 10

Звукоизоляция обычных дверей

Конструкция двери	**Условия применения**	**Звукоизоляция (дБ) на частотах, Гц**					
		125	**250**	**500**	**1000**	**2000**	**4000**
Щитовая дверь, облицованная фанерой с двух сторон	без прокладки	21	23	24	24	24	23
	с прокладкой из пористой резины	27	27	32	35	34	35
Типовая дверь П-327	без прокладки	13	23	31	33	34	36
	с прокладкой из пористой резины	29	30	31	33	34	41

Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д. Для защиты информации в особо важных помещениях используются двери с тамбуром, а также специальные двери с повышенной звукоизоляцией.

Таблица 11

Звукоизоляция специальных дверей

Конструкция двери	Звукоизоляция (дБ) на частотах, Гц					
	125	**250**	**500**	**1000**	**2000**	**4000**
Дверь звукоизолирующая облегченная	18	30	39	42	45	43
Дверь звукоизолирующа облегченная, двойная с зазором более 200 мм	25	42	55	58	60	60
Дверь звукоизолирующая тяжелая	24	36	45	51	50	49
Дверь звукоизолирующая тяжелая, двойная с зазором более 300 мм	34	46	60	60	65	65
Дверь звукоизолирующая тяжелая, двойная с облицовкой тамбура	45	58	65	70	70	70

Таблица 12

Звукоизоляция окон

Схема остекления	Звукоизоляция (дБ) на частотах, Гц					
	125	**250**	**500**	**1000**	**2000**	**4000**
Одинарное остекление:						
толщина 3 мм	17	17	22	28	31	32
толщина 4 мм	18	23	26	31	32	32
толщина 6 мм	22	22	26	30	27	25
Двойное остекл. с воздушным промежутком:						
90 мм (толщина 3 мм)	21	29	38	44	50	48
57 мм (толщина 4 мм)	21	31	38	46	49	35
90 мм (толщина 4 мм)	25	33	41	47	48	36

Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении. Существенно большую звукоизоляцию имеют окна с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или тройное комбинированное остекление. Обычные окна с двойными переплетами обладают более высокой (на 4 - 5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием. Уровень акустического сигнала за ограждением можно приближенно оценить по формуле [13;22;15]

$R_{ОГ} \approx R_C + 6 + 10 \lg S_{ОГ} - K_{ОГ}$ Дб, где R_C - уровень речевого сигнала в помещении (перед ограждением), дБ; $S_{ОГ}$ - площадь ограждения, дБ; $K_{ОГ}$- звукоизоляция ограждения, дБ. Следует иметь в виду, что в общем случае звукоизоляция ограждающих конструкций, содержащих несколько элементов, должна оцениваться звукоизоляцией наиболее слабого из них.

Таблица 13

Звукопоглощающие свойства некоторых строительных конструкций

Материал	**Толщина**	**Звукоизоляция на частотах (Гц), дБ**					
		125	**250**	**500**	**1000**	**2000**	**4000**
Кирпичная стена Отштукатуренная с двух сторон стена	½ кирпича	39	40	42	48	54	60
	1,5 кирпича	41	44	48	55	61	65
	2 кирпича	45	45	52	59	65	70
	2,5 кирпича	47	55	60	67	70	70
Стена из железобетонных блоков	40 мм	32	36	35	38	47	53
	100 мм	40	40	44	50	55	60
	200 мм	42	44	51	59	65	65
	300 мм	45	50	58	65	69	69
Стена из шлакоблоков	220 мм	42	42	48	54	60	63

При утечке акустической информации через вентиляционные воздухопроводы они ослабевают звук из-за изменения их сечения, поглощений в изгибах. Затухание в прямых металлических воздуховодах составляет 0,15 дБ/м, в неметаллических - 0.2-0.3дБ/м. При изгибах затухание достигает 3-7дБ (на один изгиб), при изменениях сечения - 1-3дБ. Ослабление сигнала на выходе из воздуховода помещения составляет 10-16дБ [13;22;15]. При среднем коэффициенте ослабления в 25 децибел обычная речь разборчиво и ясно передается через перегородку. Согласно [13;22;15] при среднем коэффициенте ослабления в 30 децибел громкая речь при отсутствии посторонних звуков довольно разборчиво слышна через перегородку. При среднем коэффициенте ослабления в 35 децибел и при отсутствии постороннего шума громкая речь слышна, но малоразборчива. При среднем коэффициенте ослабления в 40 децибел обычная речь не слышна, громкая речь немного слышна, но неразборчива; практически можно считать такую перегородку звуконепроницаемой. Простенки между квартирами должны иметь коэффициент ослабления около 40 децибел.

Защита акустического и акусто-вибрационно канала

Классификация технических средств акустической защиты [21;17;24;25;26] приведена на рис.11.

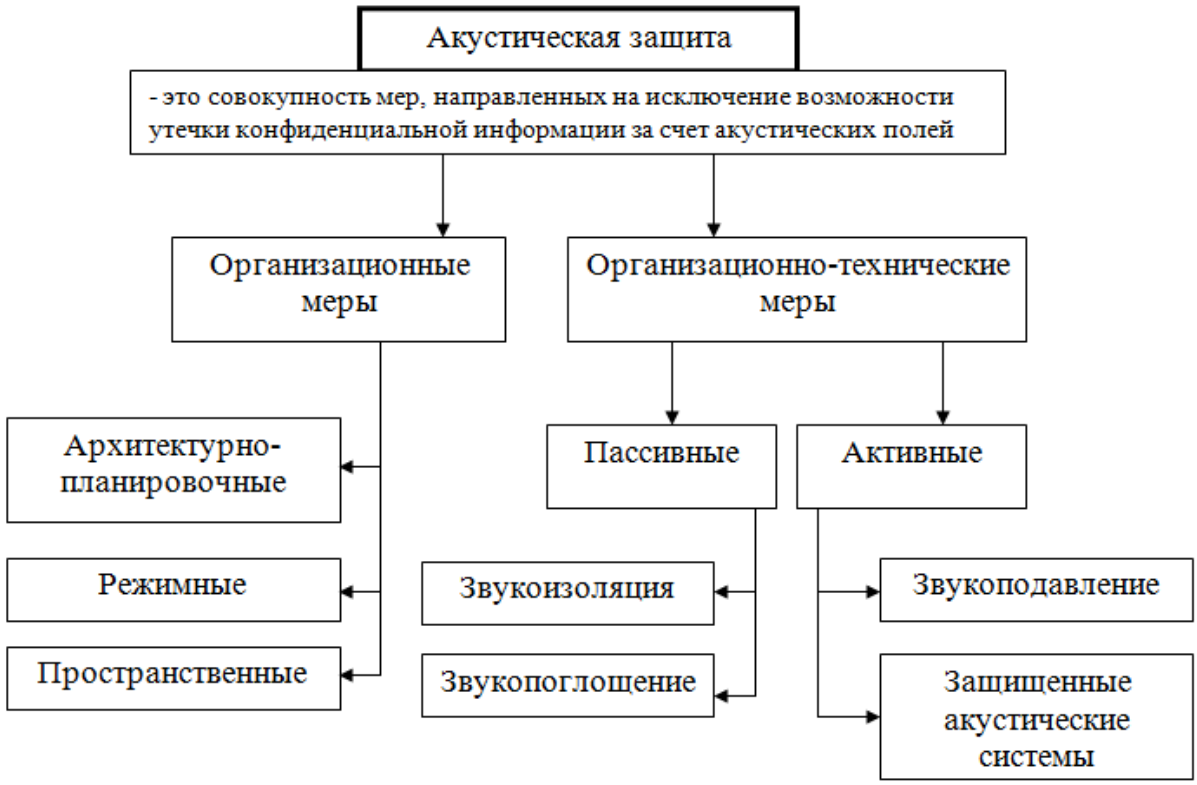


Рис.11. Классификация технических средств акустической защиты

Активная защита. Активная защита акустической информации использует аддитивную помеху [21;17;24;25;26]. При утечке акустической информации, при утечке за счет элементов строительных конструкций защищаемых помещений, уровень помехи и ее спектр должны соответствовать действующим нормативам по защите и параметрам акустического сигнала в канале утечки. При активной защите используются специальные широкополосные генераторы электрических помех в диапазоне частот речи, к которым подключаются различные излучатели, рассчитанные на создание помех а разнообразных строительных конструкциях.

В основном применяются генераторы белого и/или розового шума и системы вибрационного зашумления, имеющие в основном электромагнитные и пьезоэлектрические датчики. Качество этих систем оценивают превышением интенсивности маскирующего воздействия над уровнем акустических сигналов. Величина превышения помехи над сигналом регламентируется руководящими документами ФСТЭК [21;17;24;25;26]. Шум таковым сигналом не является, кроме того, развитие методов шумоочистки в некоторых случаях позволяет восстанавливать разборчивость речи до приемлемого уровня при значительном (20 дБ и выше)

превышении шумовой помехи над сигналом. Следовательно, для эффективного маскирования помеха должна иметь структуру речевого сообщения. Следует также отметить, что из-за психофизиологических особенностей восприятия звуковых колебаний человеком наблюдается асимметричное влияние маскирующих колебаний. Оно проявляется в том, что помеха оказывает относительно небольшое влияние на маскируемые звуки, частота которых ниже ее собственной частоты, но сильно затрудняет разборчивость более высоких по тону звуков. Поэтому для маскировки наиболее эффективны низкочастотные шумовые сигналы. Условия широкополосного согласования с ограждающими конструкциями, имеющими высокое акустическое сопротивление (кирпичная стена, бетонное перекрытие) наилучшим образом выполняются при использовании вибродатчиков с высоким механическим импендансом подвижной части, каковыми на сегодняшний день являются пьезокерамические преобразователи. Во время работы вибродатчиков возникают паразитные акустические шумы, вносящие дискомфорт и нарушающие нормальные условия труда в защищаемом помещении. Эксплуатационно-технические параметры систем виброакустического зашумления [21;17;15] приведены в таблице 14.

Таблица 14.

Эксплуатационно-технические параметры виброакустического зашумления

Характеристика	**Шорох-1**	**Шорох-2**	**ANG-2000**
Количество независимых генераторов	3	1	1
Рабочий диапазон частот, кГц	0.2…5.0	0.2…5.0	0.25…5.0
Наличие эквалайзера	Есть	Есть	Нет
Максимальное количество вибродатчиков	КВП-2-72 и КВП-7-48	КВП-2-24 и КВП-7-16	TRN-2000-18
Эффективный радиус действия стеновых вибродатчиков на перекрытии толщиной 0.25 м, м	Не менее 6 (КВП-2)	Не менее 6 (КВП-2)	5 (TRN-2000)
Эффективный радиус действия оконных вибродатчиков на стекле толщиной 4мм, м	Не менее 1.5 (КВП-7)	Не менее 1.5 (КВП-7)	-
Типы вибродатчиков	КВП-2, КВП-6, КВП-7	КВП-2, КВП-6, КВП-7	TRN-2000
Габариты вибродатчиков, мм	40x39 50x39 33x8	40x39 50x39 33x8	100x38
Возможность акустического зашумления	Есть	Есть	Есть

Увеличение мощности помехи создает повышение уровня паразитного акустического шума, что вызывает дискомфорт у работающих в помещении людей. Это приводит к отключению системы в наиболее ответственные моменты, создавая предпосылки к утечке конфиденциальных сведений.

Пассивная защита. При определенных допущениях на представление акустических сигналов в рамках диффузной теории звука требования на ослабление речевых сигналов r в каналах утечки могут быть вычислены из следующего выражения [20;21;17;15]:

$R \geq \frac{1}{2}\{L_P - L_H + D + 10\lg\left[\frac{4(1-\alpha_1)S^2}{\alpha_1{}^2 S_2^2 \alpha_2 S_2}\right]\}$, где L_p - уровень громкости речевого сигнала, определяемый уровнем звукового давления на расстоянии 1 метр от источника, α_1 - средний коэффициент поглощения звука в защищаемом помещении, S_1 - площадь внутренних поверхностей защищаемого помещения, R - звукоизолирующая способность перегородки между помещениями, α_2 - средний коэффициент поглощения звука в смежном помещении, S_2 - площадь внутренних поверхностей смежного помещения, L_H - нормативный уровень предельно допустимого звука в соответствии с санитарными требованиями, D - нормативное отношение помеха/сигнал по требованиям защиты (интегральное или в отдельных частотных полосах).

Несмотря на большое число параметров в выражении для ослабления речевого сигнала, при реальных вариациях этих параметров разброс величины ослабления незначителен. Для интегрального уровня акустических помех L_H =50 дБ (ПС-45), отношения помеха/сигнал по защите равным D =14 дБ и для уровня громкости речи L_p = 76 дБ расчеты по вариациям размеров и других параметров помещений показывают, что ослабление речевого сигнала должно составлять 14-16 дБ. Такое ослабление вполне реализуемо в большинстве практических ситуаций.

Наиболее типичными видами работ по пассивной защите являются: - заделка раствором или монтажной пеной вводов и проходов проводных, кабельных, трубопроводных и воздуховодных коммуникаций на всю толщину стены или перегородки; - установка дополнительных перегородок, разделяющих два помещения, за подвесными потолками; - установка дополнительных перегородок по ограждающим конструкциям, смежным с помещениями посторонних организаций; - усиление звукоизоляции дверных проемов с помощью дополнительных прижимных элементов или сооружением дверного тамбура.

Виброизоляция. В качестве звукоизолирующих и виброизолирующих "развязок" между различными ограждающими конструкциями и элементами ограждающих конструкций могут использоваться, к примеру, резиновые прокладки и трубчатые глушители. Резиновые прокладки, как это изображено на рис.12;13 устанавливаются в местах стыковки и под крепежом жестких элементов конструкций воздуховодов, систем отопления и водоснабжения, выходящих за пределы помещения и (или) контролируемой зоны [21;17;15].

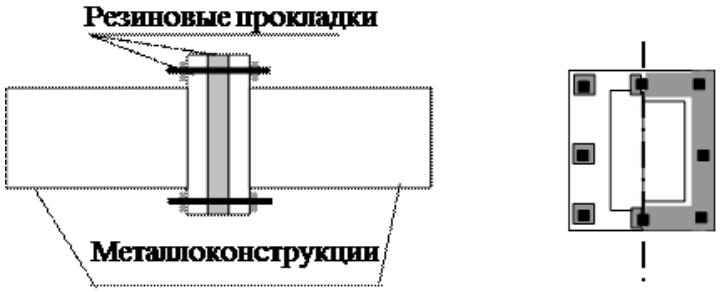


Рис.12. Виброизолирующая развязка

Применение резиновых прокладок позволяет снизить уровень сигнала в вибрационном канале на 10÷15 дБ.

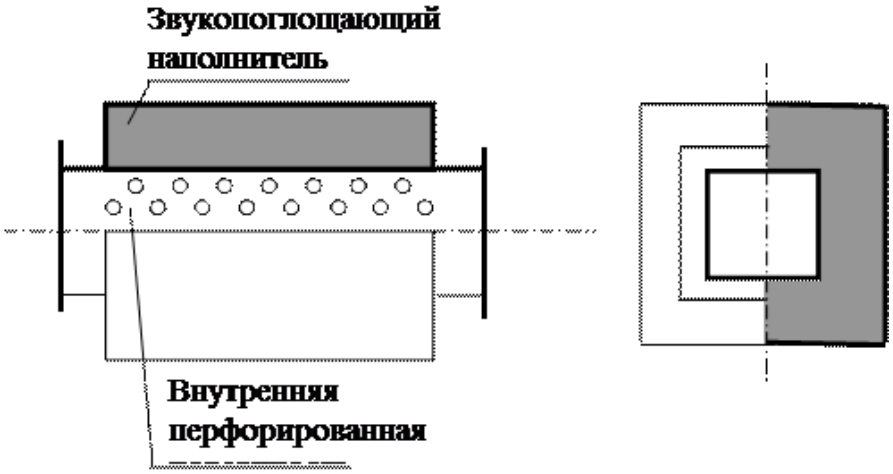


Рис.13. Конструкция трубчатого глушителя

Трубчатые глушители устанавливаются в разрыв в местах соединения металлоконструкций воздуховодов. Представляют собой облицованные звукопоглощающим материалом каналы круглого или прямоугольного сечения. Выполняются двухслойными, из оцинкованной стали. Внутренняя поверхность выполняется перфорированными листами. В качестве звукопоглощающего наполнителя могут использоваться, к примеру, минеральные ваты. Применение трубчатых глушителей позволяет внести ослабление акустического сигнала, при его распространении по воздуховоду, в среднем на 6 дБ на один метр глушителя.

Микрофоны – это преобразователи акустических колебаний в электрические. К микрофонам предъявляются высокие требования, особенно при передаче программ связанных с высокой разборчивостью, точностью, узнаваемостью информации. Размеры микрофона должны быть маленькие, а форма обтекаемой, чтобы не было нарушения однородности акустического поля. Размеры выбираются в соответствии с параметрами микрофонов. Классификация микрофонов [21;15;24;25] представлена на рис.14.

Классификация микрофонов.

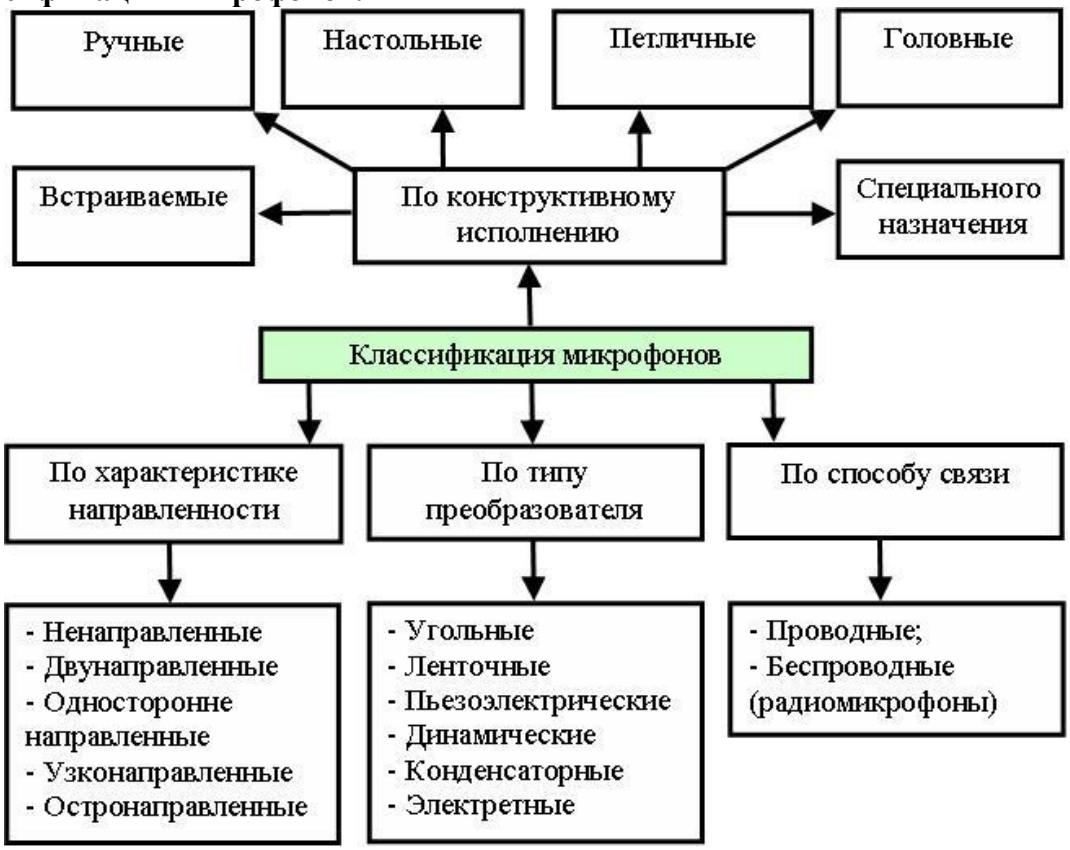


Рис.14. Классификация микрофонов

Параметры микрофонов (технические показатели качества).

Чувствительность - отношение напряжения в вольтах на выходе микрофона к звуковому давлению в Па, действующему на его вход $E = \frac{U_{вых}}{P_{ВХ}}$ Чувствительность различается для нагруженного и ненагруженного на номинальное активное сопротивление микрофона $R_{ном}$=250¸1000 Ом (в справочниках, дается для $E_{нагр}$). При измерении чувствительности, указывается при каких параметрах она измеряется. Для нахождения E в какую-либо точку поля помещают калиброванный очень малых размеров микрофон, им измеряется давление, далее в ту же точку помещают обычный микрофон и измеряют $U_{вых}$. Из отношения найденных значений получают E. Обычно оговаривается частота, на которой проводятся измерения (чаще всего 1000 Гц). Измерения проводят в свободном поле. Чувствительность зависит от многих факторов, поэтому существуют следующие величины [20;28;29]:

а) Осевая чувствительность (измерена в направлении акустической оси) $E_{ос}$.;

б) Чувствительность по диффузному полю $E = \frac{U_{вых}}{P_{ДИФ}}$;

в) Уровень чувствительности – чувствительность, выраженная в дБ относительно величины 1В/Па $L_E = 10\lg\frac{E}{E_0}$, где E_0=1 В/Па.;

г) Стандартный уровень осевой чувствительности – отношение мощности, отдаваемой в номинальную нагрузку $R_{ном}$ (при падающем звуковом давлении 1 Па) к мощности 1 мВт.

$L_{\text{СТ}} = 10lg\frac{P}{10^{-3}} = \frac{U}{R_{\text{НОМ}}10^{-3}}$, где U – напряжение на нагрузке, численно равное чувствительности микрофона при P = 1 Па.;

д) Внутреннее сопротивление микрофона Z. Обычно активное и практически не зависит от частоты. Если есть зависимость от частоты, то в справочниках обычно приводят или среднее значение, или |Z| на f = 1000 Гц;

е) Частотная характеристика чувствительности – зависимость L_E или L_{Eoc} от частоты ΔL - неравномерность частотной характеристики $\Delta L = L_{max} - L_{min}$, где L_{max} , L_{min} – max и min уровни вторичного сигнала при постоянных первичных.

Субъективно за счет неравномерности частотной характеристики происходит следующее. Если подавлены низкочастотные составляющие, то микрофон «звенит», подавлены высокочастотные составляющие – звук глухой. При подчеркивании низкочастотных составляющих микрофон «бубнит», при подчеркивании высокочастотных составляющих – «свистит». Все эти частотные искажения оцениваются по величине неравномерности частотной характеристики. Номинальный диапазон определяют по допустимым спадам чувствительности в области ВЧ и НЧ. Отклонение от горизонтальной линии в номинальном диапазоне определяют частотные искажения микрофона. При определении неравномерности частотной характеристики обычно выбирают пики которые меньше 1/8 октавы (критические полоски слуха). Для вещательных микрофонов [28;27;24] неравномерность частотной характеристики (рис.15) определяется в двух диапазонах, в номинальном и основном (основной диапазон: f=200¸5000 Гц). Вблизи границ диапазона неравномерность не должна превышать допустимых значений. Обычно аппаратура выпускается с заданной неравномерностью, если нет, то дается диапазон, в котором неравномерность не превышает заданную.

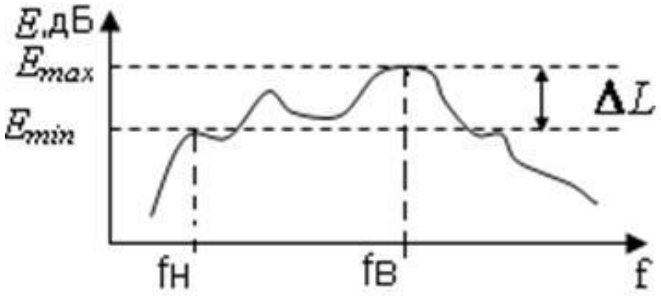


Рис.15. Частотная характеристика чувствительности.

Характеристика направленности микрофона. Это зависимость чувствительности микрофона в свободном поле от угла между направлением на источник звука и осью микрофона. - нормированная характеристика направленности $R(\theta) = \frac{E_\theta}{E_{\text{ОС}}}$. Обычно микрофоны обладают осевой симметрией. Направленный микрофон обладает определенной чувствительностью с обратной стороны, поэтому

существует понятие чувствительность «фронт - тыл». По характеристикам направленности микрофоны делятся:

-ненаправленные; -односторонненаправленные; -остронаправленные; -остроодносторонне-направленные; -двунаправленные.

Коэффициент направленности. Из-за направленности микрофона чувствительность, определенная при приходе звуковой волны к микрофону под всевозможными углами, меньше осевой чувствительности. Для учета величины этого уменьшения введен коэффициент направленности Ω, который можно определить по специальному шаблону или по формулам $\Omega = \frac{E_{ОС}^2}{E_{ДИФ}^2}$, где $E_{ОС}^2$ – квадрат осевой чувствительности в свободном поле; $E_{ДИФ}^2$ – средний из квадратов чувствительности по всем радиальным направлениям. Типовые диаграммы направленности микрофонов [28;27;15] представлены на рис.16 и таблице 15.

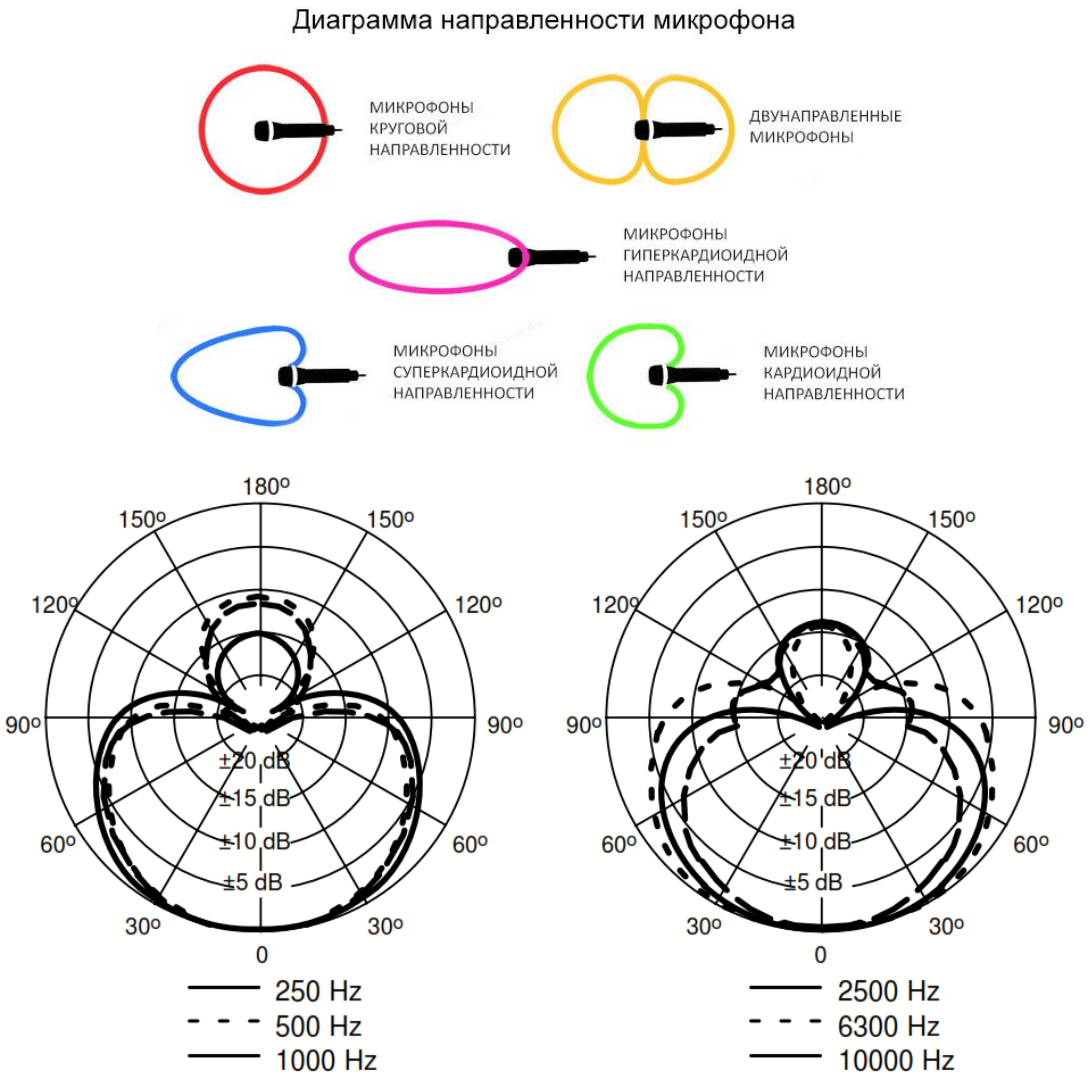


Рис.16. Диаграммы направленности микрофонов

Таблица 15

Диаграммы направленности микрофонов

Диаграмма направленности (ДН)	Коэффициент направленности Ω	Индекс направленности I, дБ	Уменьшение чувствительности сбоку, Дб
Круговая	1	0	0
Восьмерка	3	+4,7	-6
Кардиоида	3	+4,7	-6
Суперкардиоида	3,8	+5,7	-8,7
Геперкардиоида	4	+6	-12

Индекс направленности. Коэффициент направленности в дб $\mathrm{Q} = 10lg\Omega$ - показывает шумостойкость или величину подавляемого шума по отношению к сигналу. Коэффициент направленности показывает разницу в уровнях мощности развиваемых микрофоном при действии двух источников звука: одного на оси (например, голос лектора) и другого – источника рассеянных звуковых волн (шума), если они оба создают в точке микрофона одинаковое давление. Для ненаправленного микрофона этот параметр будет равен нулю, поэтому ненаправленный микрофон не подавляет шум по отношению к сигналу. Показывает величину подавления шума по отношению к сигналу, проходящему по оси микрофона.

Уровень собственного шума микрофона. Даже не включенный микрофон имеет этот параметр (тепловой, флуктуационный шумы и др.). $U_{\text{ВЫХ}} \neq 0$, даже в отсутствие сигнала. Уровень собственного шума микрофона, приведенный к акустическому входу, определяется как уровень эквивалентного звукового давления $P_ш$ при воздействии которого на микрофон, получалось бы выходное напряжение $U_ш$, равное выходному напряжению на выходе микрофона в отсутствии давления. Ниже представлены типовые характеристики микрофонов и стетоскопов [28;27;15;24].

Характеристики направленных микрофонов

Параболический микрофон:

Диаметр отражателя, м (средние значения 0,3-0,85)

Диаграмма направленности микрофона (градус) (средние значения 8-15)

Чувствительность, мВ/Па (средние значения 5-50)

Дальность перехвата разговоров, м (средние значения 50-150)

Диапазон частот, кГц (средние значения 0,1-15)

Коэффициент усиления, Дб (средние значения 30-70)

Тип питания и время работы от аккумулятора

Микрофоны «бегущей волны» (интерференционные), трубчатые микрофоны

Диапазон частот, кГц (средние значения 0,02-20)
Чувствительность, мВ/Па (средние значения 20-100)
Дальность перехвата разговоров, м (средние значения 50-100)
Коэффициент усиления, Дб (средние значения 50-90)
Размеры, мм (средние значения 229х25х13 - 500х25х250)
Тип питания и время работы от аккумулятора

Микрофонные решётки, «плоские» направленные микрофоны

Диапазон частот, кГц (средние значения 0,02-20)
Чувствительность, мВ/Па (средние значения 5-50)
Дальность перехвата разговоров, м (средние значения 100-150)
Коэффициент усиления, Дб (средние значения 40-80)
Динамический диапазон, дБА (средние значения 30-150)
Размеры решетки, мм (средние значения 175х175 – диаметр 1000)
Тип питания и время работы от аккумулятора

Лазерные микрофоны (лазерные акустические системы разведки (ЛАСР))

Тип лазера (обычно полупроводниковый)
Тип приемника (обычно малошумящий PIN-диод)
Длина волны, мкм (0,75 - 0,84; 1,75 – 1,84)
Мощность излучения, мВт (прд) (средние значения 5-25)
Фокусное расстояние объектива, мм (прд/прм) (средние значения 135/500)
Коэффициент усиления, Дб (средние значения 70-120)
Дальность перехвата разговоров, м (средние значения 100-300, при использовании триппель-призм или специальных покрытий стекла до 500-700)
Тип (приемник и передатчик совмещенный или разнесенный)
Тип питания и время работы от аккумулятора

Электронные стетоскопы

Максимальный коэффициент усиления, дБ 50- 100
Диапазон регулировки, дБ обычно ±10
Тип контактного микрофона обычно пьезомикрофон
Диапазон частот, кГц средние значения 0,3-15
Питание − встроенный аккумулятор
Время работы от аккумулятора

3.4. Основные термины, определения и технические характеристики средств защиты информации от утечки информации по радиоэлектронному каналу и ПЭМИН

Виды утечки информации. В зависимости от способа перехвата информации различают **два вида радиоэлектронного канала утечки информации.**

В канале утечки 1-го вида [4;24;29;30] производится перехват информации, передаваемой по функциональному каналу связи. С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала функционального радиоканала или подключается (контактно или дистанционно) к проводам соответствующего функционального канала. Такой канал утечки информации имеет общий с функциональным каналом источник сигналов - передатчик. Так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то среды распространения сигналов в них от общего передатчика различные или совпадают, например, до места подключения приемника злоумышленника к проводам телефонной сети.

Радиоэлектронный канал утечки 2-го вида имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов. Передатчик этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. В качестве такого передатчика применяются источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают на базе акустоэлектрических преобразователей, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Опасные сигналы создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил эксплуатации, не учете полей вокруг средств или токонесущих проводов при их прокладке в здании и т.д. Схема образования опасных сигналов [4;24;29] показана на рис.17.

Рис. 17. Схема образования опасных сигналов

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

К ОТСС относятся средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных.

В том числе технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации).

ВТСС –технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, но устанавливаемые совместно с ОТСС или в защищаемых помещениях.

ВТСС:

•Телефонные средства и системы.

•Средства вычислительной техники.

•Средства и системы передачи данных в системе радиосвязи.

•Средства и системы охранной и пожарной сигнализации.

•Средства и системы оповещения и сигнализации.

•Контрольно-измерительная аппаратура.

•Средства и системы кондиционирования.

•Средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания; телевизоры и радиоприемники и т.д.).

•Средства электронной оргтехники.

•Средства и системы электрочасофикации.

Важным понятием для технической защиты информации является **контролируемая зона** – зона (территория, здание, часть здания, помещение), в котором исключено несанкционированное пребывание сотрудников и посетителей организации, а также транспортных средств [28; 4;24;29]. Мероприятия по технической защите информации в общем случае направлены на снижение отношения сигнал-шум на **границах** контролируемой зоны во всех технических каналах утечки информации – акустических и электромагнитных. Контролируемая зона должна включать в себя опасные зоны *R1* и *R2*, чтобы исключить возможность доступа злоумышленника к информационному сигналу с мощностью достаточной для его расшифровки [28;4;24;29]. Границы контролируемой зоны могут проходить по стенам (полу и потолку) помещения или нескольких помещений, по стенам здания или по периметру охраняемой территории, прилегающей к зданию.

Опасная зона *R1* – область вокруг ТСПИ, в которой наводки на случайных антеннах выше допустимого нормированного уровня. В зоне *R1* запрещается размещение цепей ВТСС, имеющих выход электрических цепей за пределы контролируемой зоны.

Опасная зона *R2* – область вокруг ТСПИ, в которой отношение «сигнал/шум» побочных электромагнитных излучений ТСПИ превышает допустимое нормированное значение и возможен их перехват с помощью идеального приемника с последующей расшифровкой информации. Существуют две основные методики оценки защищенности ТС от утечки по каналу ПЭМИН [28; 4;24;29]. Это методика специальных исследований, результатом измерения которой является расчет радиусов *R2, r1 и r1'*, и методика оценки защищенности, результатом которой является измеренное и рассчитанное соотношение сигнал/шум на границе контролируемой зоны (реальное затухание). В первой методике расчет производится из предположения, что ЭМ-поле распространяется над полупроводящей поверхностью, и применима она соответственно в условиях, близких к этим. Вторая методика учитывает затухание от источника сигнала (в данном случае исследуемого технического средства) до границы контролируемой зоны. Однако в ее рамках не определяются радиусы зоны 1 и зоны 1' и, следовательно, она является заметно более простой. Наиболее объективной является методика определения *R2, r1 и r1'*, дополненная методом реальных зон. Выбор методики в каждом конкретном случае зависит от специалиста.

Зона 2 для каждого ОТСС определяется инструментально-расчетным методом и, как правило, указывается в эксплуатационной документации. Пространство вокруг ОТСС, в пределах которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах превышает допустимое (нормированное) значение называется **зоной 1 (*r1*)**, а в распределенных антеннах – **зоной 1' (*r1'*)**. В отличие от зоны *R2*, размер зоны *r1* (*r1'*) зависит не только от уровня побочных электромагнитных излучений ТСПИ, но и от длины случайной антенны (от помещения, в котором установлено ТСПИ до места возможного подключения к ней средства разведки).

Зоны *r1* (*r1'*) для каждого ОТСС определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия.

Для возникновения электрического канала утечки информации [28; 4;24;29] необходимо, чтобы (рис. 18):

- соединительные линии ВТСС, линии электропитания, посторонние проводники и т.д., выполняющие роль случайных антенн, выходили за пределы контролируемой зоны объекта;
- расстояние от СВТ до случайной сосредоточенной антенны было менее *r1*, а расстояние до случайной распределённой антенны было менее *r1'*;
- была возможность непосредственного подключения к случайной антенне за пределами контролируемой зоны объекта средств разведки ПЭМИН.

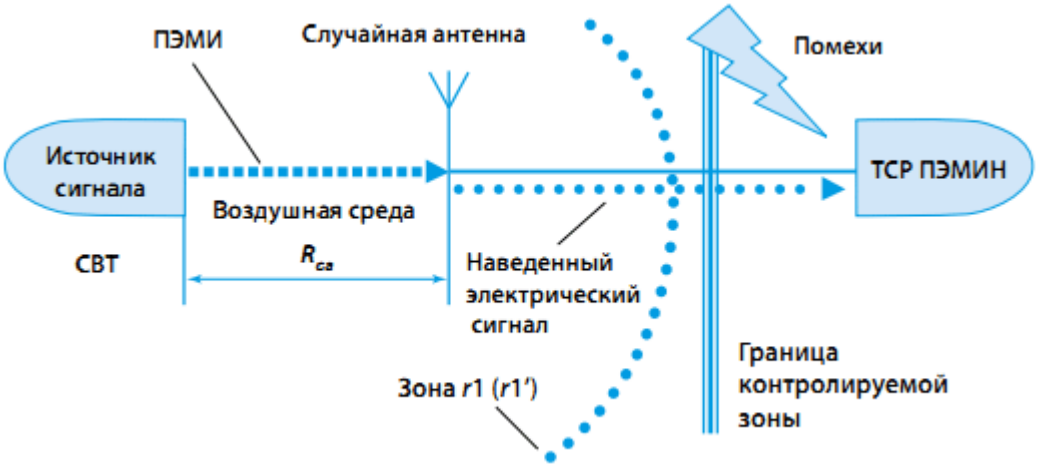


Рис.18. Схема технического канала утечки информации, возникающего за счёт наводок побочных электромагнитных излучений СВТ в случайных антеннах (схема электрического канала утечки информации)

Физическую основу случайных опасных сигналов, возникающих во время работы в выделенном помещении радиосредств и электрических приборов, составляют побочные электромагнитные излучения и наводки (ПЭМИН).

Процессы и явления, образующие ПЭМИН, по способам возникновения можно разделить на 4 вида:

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

Все разнообразие акустоэлектрических преобразователей группируется на ряд классов [15;31;32] :

-индуктивные генераторные преобразователи, работающие на основе явления электромагнитной индукции. Они подразделяются на три группы:

- электромагнитные преобразователи, содержащие магниты, их действие основано на изменении магнитного потока при движении сердечника под давлением акустического поля;

- электродинамические преобразователи, представляющие собой индукционную систему, их действие основано на электродинамическом эффекте, который проявляется в возникновении ЭДС при перемещении контура (провода) в магнитном поле под давлением силового акустического поля;

- магнитострикционные преобразователи, их действие основано на преобразовании колебания сердечника под действием внешней переменной силы звукового поля в переменную намагниченность, наводящую в обмотке переменную ЭДС.

-ёмкостные преобразователи;

-пьезоэлектрические преобразователи;

-тензорезестивные преобразователи.

Принцип действия емкостного акустоэлектрического преобразователя основан на изменении емкости конденсатора при воздействии упругой механической волны, создаваемой акустическими сигналами.

Возможны три способа изменения емкости конденсатора под действием силовых акустических волн:

1. путем изменения площади перекрытия пластин – возникает в конденсаторах переменной емкости;

2. путем изменения диэлектрической проницаемости за счет смещения диэлектрика;

3. путем изменения расстояния между пластинами конденсатора за счет сжимающего и разжимающего усилия.

Пьезоэлектрический преобразователь. Пьезоэлектрический преобразователь является генераторным преобразователем, вырабатывающим ЭДС. Пьезоэлектрический преобразователь представляет собой электрический конденсатор, состоящий из пластины пьезоэлемента, то есть кристалла из пьезоэлектрика определенных размеров и электродов из проводящего материала, наложенных на грани пластины.

Принцип действия пьезоэлектрических акустоэлектрических преобразователей основан на использовании прямого пьезоэффекта, то есть способности пьезоэлектрических материалов генерировать электрические заряды при приложении механической нагрузки производимой силовым акустическим полем. К пьезоэлектрическим материалам относятся кристаллические вещества (естественные кристаллы кварца) и специальные искусственные керамики, в которых при сжатии и растяжении в определенных направлениях возникает электрическое напряжение. Это так называемый прямой пьезоэффект, при обратном пьезоэффекте появляются механические деформации под действием электрического поля.

Примерами устройств, действующих на основе пьезоэффекта, являются источники ультразвука, излучатели и приемники звука, микрофоны и гидрофоны, звуковые резонаторы, фильтры, датчики механических напряжений.

Тензорезистивный преобразователь. Это особый класс акустоэлектрических преобразователей, к которому относятся необратимые приемники звука, принцип действия которых основан на применении электрического сопротивления чувствительного элемента, под действием механических деформаций приложенного воздействия звуковым полем.

Конструктивно большинство тензорезисторов выпускается в виде проводников, жестко связанных с бумажной или пленочной основой. Проводник представляет собой, так называемую решетку из зигзагообразно уложенной тонкой проволоки диаметром 0,02 – 0,05 мм, к концам которой пайкой или сваркой присоединяются выводные медные проводники. Сверху проводники закрываются бумагой или пленкой или покрываются лаком. После наклеивания подложки тензорезистора на поверхность, деформация этой поверхности передается проводниками и приводит к изменению их сопротивления. Наиболее распространенной измерительной цепью для тензорезисторов является мостовая измерительная схема, работающая в неравновесном режиме. Итак, механическое давление, создаваемое звуковой волной, приводит к изменению электрического сопротивления тензорезистивного преобразователя, что в свою очередь приводить изменению напряжения в диагонали мостовой схемы, то есть возникает

электрический сигнал пропорциональный изменяемой нагрузке. Качество тензорезистора определяется его коэффициентом тензочувствительности К и величиной температурного коэффициента сопротивления (ТКС). Наиболее известным акусторезистивным преобразователем является угольный микрофон.

Низкочастотные и высокочастотные излучения технических средств. При функционировании радиоэлектронных средств и электрических приборов возникают побочные излучения электромагнитных полей (ЭМ-полей), которые могут содержать защищаемую информацию. Источниками излучений [15;31;32] чаще всего являются токопроводящие цепи, содержащие статические или динамические заряды. Носители информации могут попадать в цепи непосредственно в процессе обработки информации, а также через паразитные связи. Вид излучения и характер распространения ЭМ-поля зависят от частоты колебания поля и вида излучателя. Различают низкочастотные и высокочастотные опасные излучения.

Низкочастотными считаются излучения звукового диапазона, источниками которых являются цепи и устройства звукоусилительной аппаратуры (микрофоны, аудиомагнитофоны, телефонные аппараты, кабели между этими устройствами и т.п.).

К **высокочастотным** опасным излучениям относятся электромагнитные поля, излучаемые цепями радиоэлектронных средств, по которым распространяются высокочастотные сигналы, содержащие защищаемую информацию. К основным источникам побочных излучений с мощностью, достаточной для выхода сигнала за пределы контролируемой зоны, относятся:

- гетеродины радио- и телевизионных приемников;
- генераторы подмагничивания и стирания аудио- и видеомагнитофонов;
- усилители и логические элементы в режиме паразитной генерации;
- электронно-лучевые трубки мониторов и *телевизоров*;
- элементы ВЧ-навязывания;
- элементы компьютера, в которых циркулируют сигналы в параллельном коде.

К излучающим элементам ВЧ-навязывания относятся радио- и механические элементы, которые модулируют подводимые к ним электрические и радиосигналы:

- нелинейные элементы, на которые одновременно поступают низкочастотный электрический сигнал и высокочастотный гармонический сигнал. При этом последний модулируется первым.
- токопроводящие механические конструкции, изменяющие свой размер и переотражающие внешнее ЭМ-поле.

Паразитные связи и наводки

Паразитные связи и наводки характерны для любых радиоэлектронных средств и проводов соединяющих их кабелей [27;15;31;32]. Различают три вида паразитных связей:

- гальваническая;
- индуктивная;
- емкостная.

Гальваническая связь или связь через сопротивление возникает, когда по одним и тем же цепям протекают токи разных источников сигналов. В этом случае происходит проникновение сигналов в не предназначенные для них элементы схемы.

Сигналы, несущие конфиденциальную информацию, за счет гальванической связи могут проникать в цепи, имеющие внешний выход. Это создает предпосылки для утечки информации.

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

В любом радиотехническом изделии имеется собственный блок питания, который преобразует напряжение 220 В переменного тока в требуемые для нормальной работы прибора значения напряжения постоянного и переменного тока. К примеру, для питания всех устройств ПЭВМ ее блок питания формирует напряжения +5, -5, - 12, +12 В постоянного тока.

Функциональный или опасный сигнал может при определенных условиях проникать через цепи питания прибора в сеть электропитания помещения и здания, далее через силовой щит в силовой кабель, по которому подается электроэнергия с подстанции. Вместе с тем, потребление энергии любым радиоэлектронным средством в текущий момент времени зависит от амплитуды токов, циркулирующих в нем, в том числе токов, несущих полезную информацию. Следовательно, ток, потребляемый средством, может содержать переменную составляющую, соответствующую информационному сигналу [15;31;32]. Существенное различие частот электропитания 50 Гц и речевого сигнала позволяет, в принципе, выделить с помощью частотных фильтров опасный сигнал чрезвычайно малой амплитуды на фоне напряжения 220В. Хотя блок питания сглаживает колебания тока в сети электропитания, вызванные циркулирующими в технических средствах информационными сигналами, но существует реальная возможность утечки информации через цепи питания от звукоусиливающей аппаратуры.

Цепи заземления предназначены для обеспечения зашиты электрических сигналов с информацией от помех и наводок путем экранирования проводов или устройств. При воздействии на экраны побочных электрических и электромагнитных полей на экранах возникают заряды, которые для эффективного экранирования крайне важно удалять или нейтрализовать. С этой целью экраны «заземляют», т. е. соединяют проводом с малым сопротивлением с поверхностью Земли [4;15]. В качестве «земли» применяют металлические листы или трубы, зарытые в грунт на глубину 1-2 м для обеспечения хорошего контакта с токопроводящими слоями. Протекающие по цепи заземления опасные сигналы могут перехватываться приемной аппаратурой злоумышленника.

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

Паразитная индуктивная связь проявляется следующим образом. В пространстве, окружающем любую цепь, по которой протекает электрический ток *I,* возникает магнитное поле, постоянное или переменное с частотой изменения тока w. В соседних проводниках, находящихся в переменном магнитном поле, возникают

ЭДС $E = Iw M$, где M — взаимная индуктивность. Величина M пропорциональна индуктивности влияющих друг на друга элементов цепей и обратно пропорциональна расстояния между ними [15;31]. К примеру, взаимно-индуктивность двух прямых медных параллельных проводников длиной 100мм и толщиной 0.02 мм при интервале между ними 2 мм составляет 0.07 мкГн, а при интервале 10 мм — 0.04 мкГн.

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

Из-за паразитных индуктивных и емкостных связей возникают паразитные наводки. Под паразитной наводкой принято понимать передача электрических сигналов из одного элемента радиоустройства в другой, не предусмотренная его схемой и конструкцией [27;30].

Когда ток проходит по проводникам первой цепи (Ц1), вокруг них создается магнитное поле, силовые линии которого пронизывают проводники второй цепи (Ц2). В результате этого по цепи Ц2 потечет помимо основного еще и переходной ток, создающий помеху основному. Защищенность от взаимных помех оценивается так называемым переходным затуханием

$Z_{12}=10\lg P_{C1}/P_{H2}$, где P_{C1} и P_{H2} — мощность сигналов в 1-й цепи и наводки от них во 2-й цепи. Переходное затухание для надежной защиты информации должно быть не менее величины $10\lg P_C/P_{пр}$, где P_C и $P_{пр}$ — мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал.

Наводки создают угрозу безопасности информации в случае наводок на цепи, имеющие выход сигналов с подлежащей защите информацией за пределы территории организации. В этом отношении наибольшую угрозу создают наводки в проводах кабелей городской телефонной сети, радиотрансляции, электропитания от сигналов рядом расположенных кабелей внутренней АТС, звукофикации залов или помещений для совещаний, оперативной и диспетчерской связи. Вместе с тем, наводки даже очень малого уровня могут модулировать высокочастотный сигнал, распространяющийся за пределы организации в виде электромагнитной волны [15;31].

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС- линейное зашумление [15;31]. К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования [15;31]:

• система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

• создаваемые помехи не должны иметь регулярной структуры;

• уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой

зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;

• система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);

• на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по ЭМС.

Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ.

В системах пространственного зашумления в основном используются помехи типа "белого шума" или "синфазные помехи" [15;31]. Системы, реализующие метод "синфазной помехи", в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует "имитационную помеху", по спектральному составу соответствующую скрываемому сигналу.

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д. Классификация акустических радиопередающий закладных устройств по [4;15;30] представлена в таблице 16.

Таблица 16

Классификация акустических радиопередающий закладных устройств

№ п/п	Наименование показателей классификации	Значение показателей классификации
1	Вид датчика	- микрофон; -вибродатчик (контактный)
2	Вид исполнения	- обычный (модульный); - камуфлированный
3	Место установки	- в интерьере помещения; - в конструкции здания; - в электрорадиоприборах и сети 220В; - в аппаратуре ВТСС и соед. линиях
4	Способ передачи информации	- по радиоканалу; - по оптическому каналу (ИК-диапазон); - по сети электропитания (220В); - по тлф. линии и цепям коммуникаций; - по элементам строит. Конструкций (вибрация)

Окончание таблицы 16

№ п/п	Наименование показателей классификации	Значение показателей классификации
5	Вид используемых сигналов	- с простыми сигналами (АМ,ЧМ модуляция); - со сложными сигналами (ШПС, сл. фазой и пр.); - с псевдослучайной перестройкой частоты (ППРЧ)
6	Тип источника питания	- 220В; -автономное питания; - тлф. линии и цепей коммуникаций; - от источника радиоизлучения
7	Способ управления включением передатчика	- не управляемые; - с автопуском (акустоматы); - с дистанционным управлением; - автопуск по таймеру
8	Способ накопления информации	- без накопления; - с накоплением (коротким и длительным накоплением)
9	Способ кодирования информации	- без кодирования; - с аналоговым скреблированием; - с цифровым шифрованием
10	Тип стабилизации частоты передатчика	- без стабилизации; - с использованием стабилизации; -с кварцевой стабилизацией
11	Используемый диапазон длин волн	- LF низкочастотный (километровые волны); - MF среднечастотный (гектометровые волны); - HF высокочастотный (декаметровые волны); - VHF очень высокочастотный (метровые волны); - UHF ультравысокочастотный (дециметровые волны); - SHF сверхвысокочастотный (сантиметровые волны).

Высокочастотное навязывание. Методы ВЧ навязывания [27;4;15] представлены на рис.19. Перехват обрабатываемой техническими средствами информации может осуществляться путем специальных воздействий на элементы технических средств. Одним из методов такого воздействия является высокочастотное навязывание, т. е. воздействие на технические средства высокочастотных сигналов. В настоящее время используются два способа высокочастотного навязывания: - посредством контактного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством; - путем излучения высокочастотного электромагнитного поля. Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальные сведения. В результате взаимодействия на таких элементах высокочастотные навязываемые колебания оказываются промодулированными низкочастотными опасными сигналами [27;4;15].

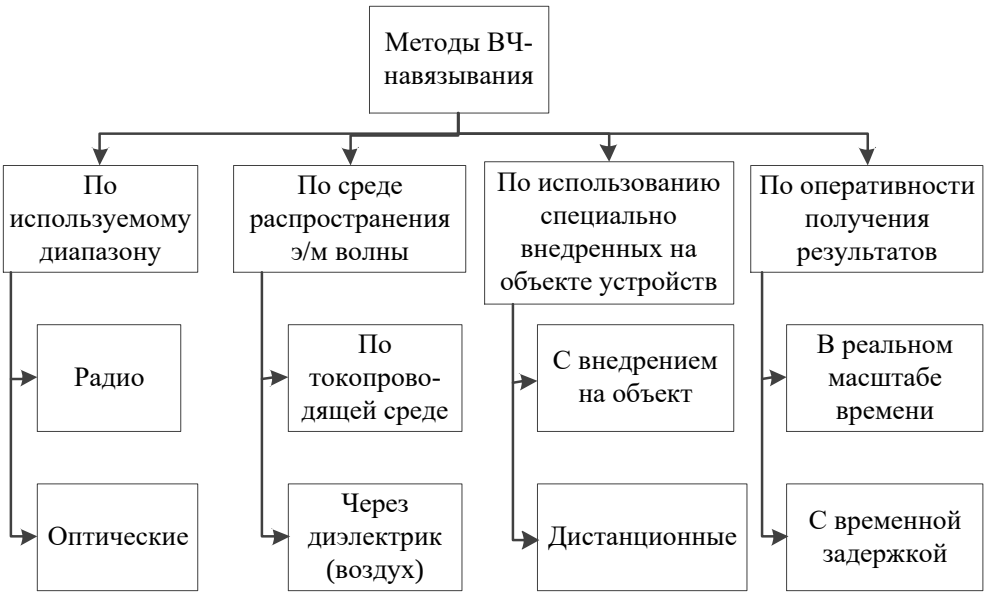


Рис.19. Методы ВЧ навязывания

Пассивные и полуактивные закладки

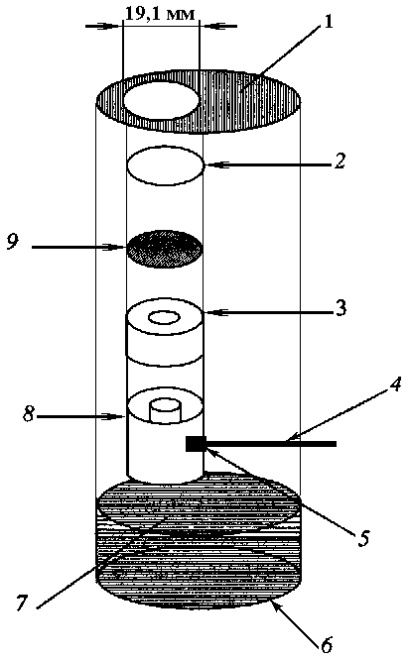


Рис.20. Пассивный радиомикрофон

На рис.20 обозначены основные элементы пассивного радиомикрофона [20;23;27]: 1 - верхняя пластмассовая крышка; 2 - ферритовое кольцо; 3 - изолятор; 4-антенна (четвертьволновой вибратор); 5 - согласующий конденсатор; 6 - корпус; 7 - жидкость; 8 - медный цилиндр (индуктивность); 9 - металлическая диафрагма.

Основой устройства является цилиндрический объемный резонатор, на дне которого налит небольшой слой масла. Верхняя часть закрыта крышкой из пластмассы, являющейся радиопрозрачной для радиоволн, но препятствующей проникновению акустических колебаний. В крышке имеется отверстие, через него внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости подобраны таким образом, чтобы вся система резонировала на внешнее излучение с частотой 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на характеристики переизлученного поля, создаваемого внутренним вибратором. Сигнал становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, то есть 330 МГц.

Наряду с пассивными закладками, аналогичными выше описанной, для съема информации используются и полуактивные закладки [27;4;15], называемые аудиотранспондерами; (Audiotransponder). Транспондеры начинают работать только при облучении их мощным узкополосным высокочастотным зондирующим (опорным) сигналом. В качестве модулирующего используется сигнал, поступающий или непосредственно с микрофона, или с микрофонного усилителя. Промодулированный ВЧ-сигнал переизлучается, при этом его частота смещается относительно несущей частоты зондирующего сигнала. Время работы транспондеров составляет несколько месяцев, так как потребляемый ток незначителен.

Основные характеристики радиозакладных акустических закладок, а также полуактивных, сетевых и инфракрасных закладок приведены в Приложении 1,2.

Технические характеристики и термины радиоприемной аппаратуры

Радиоприёмные устройства делятся по следующим признакам [10;11;5-7]:

- по основному назначению: радиовещательные, телевизионные, связные, пеленгационные, радиолокационные, для систем радиоуправления, измерительные и др.;
- по роду работы: радиотелеграфные, радиотелефонные, фототелеграфные и т. д.;
- по виду модуляции, применяемой в канале связи: амплитудная, частотная, фазовая, однополосная (разные виды), импульсная (разные виды);
- по диапазону принимаемых волн, согласно рекомендациям МККР:
  - мириаметровые волны — 100-10 км, (3 кГц-30 кГц), СДВ;
  - километровые волны — 10-1 км, (30 кГц-300 кГц), ДВ;
  - гектометровые волны — 1000—100 м, (300 кГц-3 МГц), СВ;
  - декаметровые волны — 100-10 м, (3 МГц-30 МГц), КВ;
  - метровые волны — 10-1 м, (30 МГц-300 МГц), УКВ;
  - дециметровые волны — 100-10 см, (300 МГц-3 ГГц), ДМВ;
  - сантиметровые волны — 10-1 см, (3 ГГц-30 ГГц), СМВ;
  - миллиметровые волны — 10-1 мм, (30 ГГц-300 ГГц), ММВ;

приёмник, включающий все широковещательные диапазоны (ДВ, СВ, КВ, УКВ) называют всеволновым;

- по принципу построения приёмного тракта: детекторные, прямого усиления, прямого преобразования, регенеративные, сверхрегенераторы, супергетеродинные с однократным, двукратным или многократным преобразованием частоты;
- по способу обработки сигнала: аналоговые и цифровые;
- по применённой элементной базе: на кристаллическом детекторе, ламповые, транзисторные, на микросхемах;
- по исполнению: автономные и встроенные (в состав др. устройства);
- по месту установки: стационарные, носимые;
- по способу питания: сетевое, автономное или универсальное.

Основные электрические параметры радиоприемной аппаратуры:

- диапазон рабочих частот;
- чувствительность;
- избирательность;
- частотная точность;
- динамический диапазон;
- выходная мощность и другие.

Диапазон рабочих частот. Это та область рабочих частот, в которой РПУ может плавно или скачком перестраиваться с одной частоты на другую [10;11]. При плавной перестройке задается $F_{o\ min}$ и $F_{o\ max}$, то есть нижняя и верхняя границы диапазона. Относительною ширину диапазона характеризует коэффициент перекрытия $К_д$: $К_д = F_{o\ max} / F_{o\ min}$

Для обеспечения большего $К_д$, Диапазон разбивают на части – поддиапазоны и определяют коэффициент перекрытия по поддиапазону: $К_{диап} = F_{диап\ max} / F_{диап\ min}$

Коэффициент перекрытия по поддиапазону ограничен конструкцией конденсатора переменной емкости у которого C_{max} / C_{min} = 25...50 и при этом $K_{ПД} = \sqrt{C_{max}/C_{min}} \approx 5 \dots 7$

С учётом паразитных емкостей, которые увеличивают C_{min}, коэффициент перекрытия обычно принимают равным 2...3, причем, чем выше частота принимаемого сигнала, тем меньше коэффициент перекрытия.

Чувствительность. Это способность РПУ обеспечить нормальную работу при наименьшем уровне сигнала на входе [10;11]: - милливольты и милливатты – для приема на внешние антенны в диапазоне метровых волн; - микровольты и микроватты – для приема на внешние антенны в диапазоне дециметровых волн; - для приема на магнитные антенны чуствительность измеряется в единицах напряженности поля в точке приема – милливольт на метр или микровольт на метр (mV*m, m V*m).

Зная напряженность поля в точке приема $\mathbf{E_п}$ и действующую высоту магнитной антенны $h_д$ можно вычислить теоретическую чувствительность РПУ, то есть ЭДС сигнала в антенне: $E_а = E_п * h_д$

Однако, теоретическая чувствительность РПУ снижается из-за влияния собственных шумов РПУ, ширины полосы пропускания, вида принимаемого сигнала, нелинейных явлений в каскадах. Поэтому, для оценки качества РПУ пользуются понятиями «Реальная» чувствительность и «Предельная» чувствительность.

Реальная чувствительность – это наименьшая ЭДС сигнала в антенне, при которой обеспечивается нормальная выходная мощность при заданном соотношении сигнал/шум. Нормальная выходная мощность – 10% от номинальной мощности сигнала на выходе приемника. Заданное соотношение сигнал/шум определяется видом принимаемого сигнала. Например, соотношение мощности сигнала к мощности шума для РПУ: радиовещания 50...1000; радиолокации 0,5..10; радиотелефонии 3.....10.

Реальная чувствительность зависит от режима работы детектора, субъективных свойств оператора (“глухой” радист) и неудобна с практической точки зрения для оценки РПУ с различными трактами, поэтому для оценки РПУ используют величину Предельной чувствительности – наименьшую ЭДС в антенне при соотношении сигнал/шум = 1.

Избирательность. Избирательностью (селективностью) радиоприемного устройства называется его способность выделять из различных сигналов, отличающихся по частоте, сигнал принимаемой станции [10;11]. В соответствии с этим избирательность приемника оценивается как относительное ослабление сигналов посторонних радиостанций, работающих на различных волнах, по отношению к сигналам принимаемого передатчика, на волну которого этот приемник настроен. Избирательность осуществляется главным образом входящими в состав приемника колебательными контурами и фильтрами [10;11]. Понятие избирательности поясняет рис.21, на котором показан спектр частот трех радиостанций, из которых две крайние мы рассматриваем как помехи.

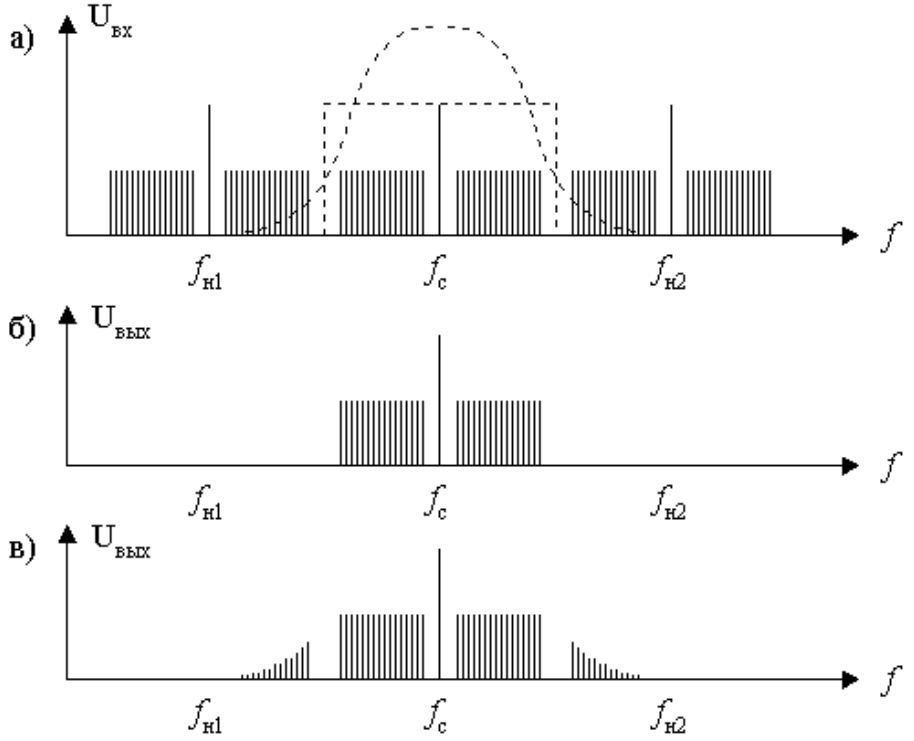


Рис.21. К пояснению избирательности радиоприемника

Из рис.21 видно, что если фильтры приемника обладают прямоугольной частотной характеристикой, соседние (мешающие) радиостанции не создадут на его

выходе никакого сигнала (рис.21б). Если же частотная характеристика фильтра далека от идеальной, то на его выходе кроме полезного сигнала будет прослушиваться помеха (рис.21 в). Естественно, что наибольшие трудности представляет ослабление помех от ближайших по частоте посторонних сигналов, т.е. сигналов соседнего частотного канала. Поэтому для оценки качества приемника всегда определяется его селективность в отношении помех соседнего канала [10;11] .

В первом приближении количественную оценку избирательности можно производить по резонансной характеристике приемника, изображающей зависимость коэффициента усиления от частоты колебаний в антенне [10;11]. Благодаря применению колебательных контуров и фильтров резонансная характеристика при настройке приемника на какую-либо частоту сигнала имеет вид, подобный рис.22.

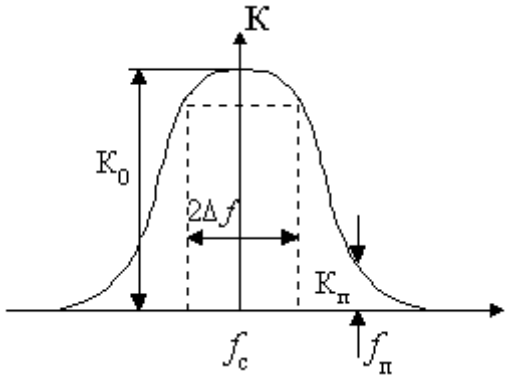


Рис.22. Резонансная характеристика приемника

Избирательность в отношении помехи на частоте f_c определяется в этом случае как $S_e = K_o/K_П$, где K_0 – коэффициент усиления на частоте настройки; $K_п$ – коэффициент усиления на частоте $f_п$. Селективность удобно определять также в децибелах: $S_{e\,дБ} = 20lgS_e = K_{o\,дБ} - K_{П\,дб}$.

Так как передаваемое сообщение имеет определенную полосу частот, другой не менее важной функцией приемника является прием сигнала высокой частоты со всеми его боковыми частотами, т.е. одновременный прием определенной полосы частот. При этом необходимо, чтобы соотношения между амплитудами составляющих спектра сигнала оставались без изменений. Последнее можно обеспечить лишь при постоянной чувствительности приемника в определенной полосе частот. Поэтому понятно, что идеальная амплитудная частотная характеристика (АЧХ) приемника должна быть прямоугольной. При такой форме приемник одинаково принимает спектр боковых частот полезного сигнала, т.е. полоса пропускания такого устройства однозначно определяется как $2\Delta_f$. Одновременно приемник с такой АЧХ обладал бы идеальной избирательностью, поскольку не пропускал бы сигналов мешающих станций и помех, частоты которых отличаются на Δ_f.

Частотная характеристика реального приемника отличается от прямоугольной. Полосой пропускания в данном случае называют область частот, в пределах которой ослабление спектра принимаемых колебаний не превышает заданного значения. Считается, что искажения будут не заметны на слух, если неравномерность АЧХ в пределах полосы пропускания не превышает 3 дБ. Это соответствует уровню 0,707.

Именно на этом уровне отсчитывается полоса пропускания. Частотные свойства контура могут быть заданы его добротностью $Q = f_0/2\Delta f$.

Качество воспроизведения принятого сигнала зависит от различного рода искажений сигнала в отдельных каскадах приемника. К этим искажениям относятся частотные, фазовые и нелинейные. На качество принятого сигнала будут влиять также различного рода помехи: атмосферные, промышленные, помехи от соседних по частоте передатчиков, а в диапазонах УКВ - собственные шумы приемника.

Частотная точность настройки и ее стабильность. Частотная точность определяет возможность вхождения в связь в установленное время без поиска сигнала корреспондента, а так же ведение связи без подстройки приемника при сохранении заданного качества воспроизведения сообщения в течении всего сеанса связи [10;11].

Частотная точность как показатель – это разность между частотой настройки приемника и частотой принимаемого сигнала. Для характеристики частотной точности используют так же величину относительной расстройки, представляющую собой отношение разности между частотами сигнала и настройки приемника к частоте сигнала : $\frac{f_0 - f_C}{f_C} = \pm\frac{\Delta f}{f_C}$

Нестабильность настройки РПУ во время работы оценивается изменением частоты настройки за определенный промежуток времени [10;11]. Например, при нестабильности 10с , где t = -8, уход частоты за сутки составит f_o/10с , где t = 8. Например, при частоте 30 МГц уход составит 0,3 Гц в сутки.

Динамический диапазон. Изменение амплитуд сигналов и помех в реальных условиях может достигать 80 дБ и более из-за влияния замираний, при изменении расстояния объектами (приемником и передатчиком). Пределы, в которых изменяется величина сигнала на входе РПУ, называется динамическим диапазоном [16;17].

Количественной оценкой динамического диапазона является коэффициент, называемый “динамический диапазон”:

$$D_{\text{СИГН}} = 10\lg\left(\frac{P_{\text{СИГН }MAX}}{P_{\text{СИГН }MIN}}\right) = 20\lg\left(\frac{U_{\text{СИГН }MAX}}{U_{\text{СИГН }MIN}}\right)$$

Увеличение величины входного сигнала приводит к перегрузке ТРЧ (тракта радиочастоты), снижению избирательности, так как ТРЧ начинает работать в нелинейном режиме и при усилении сигнала в этом случае появляются комбинационные составляющие. Избежать этого можно, если отрегулировать динамический диапазон в пределах линейного участка динамической характеристики РПУ. Для количественной оценки линейности динамического диапазона вводят понятие **Рабочего Динамического Диапазона**: $D_P = 20\lg\left(\frac{E_{a\,MAX\,\text{ДОП}}}{E_{a\,\text{П}}}\right)$, где: $E_{ап}$ – предельная чуствительность РПУ; $E_{a\ max\ доп}$ - максимально допустимая ЭДС сигнала на входе РПУ. Очевидно, что рабочий динамический диапазон D_p должен быть больше или равен D_c. Для этого в РПУ применяют АРУ и РРУ (Автоматическую и Ручную Регулировку Усиления), что позволяет уменьшить пределы изменения выходной мощности РПУ.

Выходная мощность. Это мощность, подводимая с выхода РПУ ко входу оконечного устройства. Выходная мощность $P_{вых}$ должна быть номинальной для данного конкретного типа оконечного устройства ОУ и колеблется от долей ватта до

нескольких ватт [10;11]. Различают **нормальную** и **номинальную** выходную мощность.

Номинальная выходная мощность – это наибольшая выходная мощность, при которой возникающие нелинейные искажения не превышают заданной величины. Номинальная выходная мощность соответствует 100% модуляции принимаемого сигнала. **Нормальная** выходная мощность соответствует 10% от номинальной, 30% модуляции сигнала и подводится к оконечному устройству при измерении характеристик РПУ.

В значительной степени качество воспроизведения принятых сигналов зависит и **от нелинейных искажений.**

Нелинейными называются искажения, которые проявляются в том, что в воспроизводимом звуке появляются дополнительные звуки, изменяющие тембр звука [10;11]. Эти искажения проявляются обычно в виде хрипов и дребезжаний, искажающих воспроизводимую передачу. Главной причиной появления нелинейных искажений является нелинейность ламповых характеристик. Кроме того, они возникают из-за нелинейности кривой намагничивания стали, из которой выполнен междуламповый или выходной трансформатор. Наибольшие искажения возникают, как правило, в оконечных каскадах усилителей низкой частоты.

Установлено, что наше ухо совсем не замечает нелинейных искажений, коэффициент которых не превышает 3—5%. Такому условию удовлетворяют высококачественные приемники и усилители. В более простых приемниках коэффициент нелинейных искажений может составлять 7—8%.

Соотношение сигнал/шум. Отношение "сигнал/шум" (SNR) - это отношение среднеквадратического значения величины входного сигнала к среднеквадратическому значению величины шума (за исключением гармонических искажений), выраженное в децибелах [16;17] $SNR(dB) = 20 \log [V_{signal(rms)}/ V_{noise(rms)}]$. Это значение позволяет определить долю шума в измеряемом сигнале по отношению к полезному сигналу.

Технические характеристики и термины радиосканеров

Технические характеристики и типы сканирования радиосканеров [10;11].

В целом сканирующие радиоприемники характеризуются следующими показателями:

•диапазоном принимаемых частот:

• чувствительностью;

• избирательностью;

• параметрами сканирования (скоростью перестройки, шаг сканирования, полосами обзора и т.д.);

• используемым методом или методами, если они есть, обнаружения сигналов;

• видом принимаемых радиосигналов;

•оперативностью управления и возможностями его автоматизации;

• выходными параметрами, такими, как качество воспроизведения сигнала на выходе приемника, наличие выходов по промежуточной и низкой частоте, значения полос пропускания сигнала по этим частотам и т.д.;

•эксплуатационными параметрами (массогабаритные характеристики, требования по электропитанию, надежность, ремонтопригодность, удобство транспортировки и т.п.).

Типы сканирования радиосканеров могут варьироваться в зависимости от выбранной модели. Например:

all with save new - сканирование всех частот в диапазоне с занесением вновь найденных в таблицу.

all without save new - сканирование всех частот в диапазоне без занесения вновь найденных в таблицу.

only memorized except new - сканирование по частотам сохраненным в менеджере частот.

only new except memorized - сканирование только новых частот, сохраненные в менеджере частоты игнорируются

Сканирование каналов памяти одного вида модуляции (mode scan).

При обнаружении сигнала на канале приемник в зависимости от настройки:

• остается на канале до момента прекращения сигнала и продолжает сканировать через 2 секунды после его прекращения

• остается на канале от 1 до 12 секунд (по умолчанию — 5), после чего продолжает сканирование

• полностью прекращает сканирование

Технические характеристики и термины радиопеленгаторов

К наиболее важным техническим характеристикам радиопеленгаторов [8;19;15] относятся: - вид пеленгуемого сигнала, - диапазон рабочих частот, - точность пеленгования, - чувствительность, - помехоустойчивость, - быстродействие, - разрешающая способность, - время развертывания, - масса и габариты.

Технические характеристики и термины радиопередающей аппаратуры

Основным показателям радиопередатчика [10;11] относятся: диапазон волн, мощность, коэффициент полезного действия, вид и качество передаваемых сигналов. В соответствии с классификацией радиоволн различают передатчики километровых, гектометровых, декаметровых и других волн. С этим различием связаны соответствующие особенности конструкций, так как в разных диапазонах различны конструкции колебательных контуров и типов усилительных эле ментов. Передатчик может работать на одной или нескольких выделенных для него фиксированных волнах, либо он может настраиваться на любую длину волны в непрерывном диапазоне волн.

Мощность передатчика обычно определяется как максимальная мощность высокочастотных колебаний, поступающая в антенну при отсутствии модуляции и при непрерывном излучении [10;11]. Однако этой характеристики недостаточно для оценки мощности радиопередатчика. Дело в том, что в технике радиосвязи часто приходится иметь дело с сигналами, напряжение которых изменяется в очень широких пределах и в сравнительно короткие промежутки времени может принимать значения, в несколько раз превосходящие средний уровень. Характерным примером подобного режима может служить радиолокационный передатчик, излучающий импульсы длительностью около 1 микросекунды, разделенные интервалами около 1 миллисекунды, т.е. в 1000 раз большей длительности. Если бы при проектировании передатчика расчет велся на то, что в моменты этих выбросов мощность излучения соответствовала бы номинальной,

то фактическая средняя мощность излучения была бы во много раз меньше. Передатчик был бы использован значительно слабее своих возможностей, а при необходимости обеспечить большую дальность радиосвязи потребовалось бы применить передатчик значительно большей мощности.

В системах радиовещания промежутки времени, в которые амплитуда колебаний достигает максимальных значений, занимают обычно большую часть общего времени работы передатчика (например, 10…20%), длительность их доходит до десятков миллисекунд, но ив этом случае описанное временное форсирование передатчика возможно, хотя и в меньших пределах [10;11].

В соответствии с изложенным мощность передатчика, помимо цифры максимальной мощности, при непрерывной работе характеризуют значениями пиковой мощности, которая может быть обеспечена в течение ограниченных промежутков времени. Например, если средняя мощность передатчика при непрерывной работе 100 кВт, то она может доходить до 200 кВт, если длительность импульсов не превышает интервалов между ними.

Важнейшими показателями радиопередатчика являются стабильность излучаемой им частоты и уровень побочных излучений [10;11]. Дело в том, что если строго соблюдается присвоенная данному передатчику частота сигнала, то настроенный на эту частоту приемник начинает принимать передаваемые сигналы тотчас после включения, не требуя подстроек; это способствует удобству эксплуатации и высокой надежности радиосвязи, а также облегчает автоматизацию оборудования. Кроме того, частотные диапазоны, используемые для радиосвязи и вещания, переуплотнены сигналами одновременно работающих радиостанций, поэтому если частота передатчика отличается от разрешенного значения, то она может приблизиться к частоте другого передатчика, что вызовет помехи приему его сигналов.

По существующим международным нормам отклонение от номинала частоты передатчика для радиосвязи на гектометровых волнах не должно превышать 0,005%; для радиовещательных передатчиков отклонение частоты-в этом диапазоне не должно превышать 10 Гц [10;11]. На декаметровых волнах допустимая нестабильность частоты для передатчиков мощностью более 0,5 кВт равна $15 \cdot 10^{-6}$, что соответствует в диапазоне 4…30 МГц абсолютному отклонению частоты от 60 до 450 Гц. Некоторые системы радиосвязи по своему принципу работы требуют, чтобы стабильность частоты была значительно лучше, чем предусматривается указанными нормами [10;11].

Побочными излучениями радиопередатчика называются излучения на частотах, расположенных за пределами полосы, которую занимает передаваемый радиосигнал. К побочным излучениям относятся гармонические излучения передатчика, паразитные излучения и вредные продукты взаимной модуляции [10;11].

Гармоническими излучениями (гармониками) передатчика называются излучения на частотах, в целое число раз превышающих частоту передаваемого радиосигнала.

Паразитными излучениями называются возникающие иногда в передатчиках колебания, частоты которых никак не связаны с частотой радиосигнала или с частотами вспомогательных колебаний, используемых в процессе синтеза частот, модуляции и других процессов обработки сигнала [10;11].

Известно, что при действии в нелинейной цепи, например, двух ЭДС с частотами f_1 и f_2, спектр тока содержит, помимо составляющих с этими частотами и их гармоник, также составляющие с частотами вида mf1 ±nf$_2$, где m и п — целые числа. Это явление и лежит в основе взаимной модуляции; оно обусловлено наличием в передатчике элементов, обладающих нелинейными характеристиками, главным образом транзисторов или электронных ламп.

Интенсивность побочных излучений характеризуется мощностью соответствующих колебаний в антенне передатчика. Например, по: действующим международным нормам радиопередатчики на частотах до 30 МГц должны иметь мощность побочных излучений не менее чем в 10000 раз (на 40 дБ) ниже мощности основного излучения и не более 50 мВт [10;11].

Показатели, определяющие качество передачи вещательного сигнала (электроакустические показатели), в принципе не отличаются от аналогичных параметров электрического канала вещания, что естественно, поскольку передатчик является частью канала — трактом вторичного распределения. Некоторое отличие заключается лишь в том, что эти показатели нормируются и измеряются относительно уровня сигнала, соответствующего определенному коэффициенту модуляции сигналом частотой 1000 Гц. Для допустимого отклонения амплитудно-частотной характеристики этот коэффициент равен 50%.

Коэффициент гармоник определяется при коэффициенте модуляции 50, 90, а также 10%, что обусловлено наличием в модуляторе передатчика специфических искажений вида двустороннего ограничения, заметных при большом коэффициенте модуляции, вида «центральной отсечки», заметных при малом коэффициенте модуляции [10;11]. Защищенность от интегральной помехи и от псофометрического шума измеряется относительно уровня модулирующего сигнала, соответствующего 100%-ной модуляции. Эксплуатационный персонал часто употребляет термин «уровень шумов», который оценивается в децибелах относительно уровня модулирующего сигнала с частотой 1000 Гц, соответствующего коэффициенту модуляции 100%. Численно он равен величине защищенности от интегральной помехи, взятой со знаком «минус».

Радиопередатчики можно классифицировать по назначению, по диапазону волн, по мощности, по роду работы, способу транспортировки [10;11]. Так, в зависимости от назначения передатчики делятся на связные, радиовещательные, телевизионные, радиолокационные, радионавигационные, телеметрические и т.д. По мощности передатчики подразделяются на маломощные (до 100 Вт), средней мощности (до 10 кВт), мощные (до 1000 кВт) и сверхмощные (свыше 1000 кВт). По роду работы (виду излучения) различают передатчики телеграфные, телефонные, однополосные, импульсные и т.д. По способу транспортировки передатчики классифицируются на стационарные и подвижные (переносные, автомобильные, самолетные и т.д.).

Специальные обозначения выражение единиц мощности в децибелах:

Если в качестве одной из величин отношения (в знаменателе) выступает общепринятая исходная (или опорная) величина X_{ref}, то отношение, выраженное в

децибелах, называют *уровнем* (иногда называют *абсолютным уровнем*) соответствующей физической величины *X* и обозначают L_X (от англ. *level*).

В соответствии с действующими стандартами, при необходимости указать исходную величину её значение помещают в скобках за обозначением логарифмической величины [10;11]. Например, уровень L_P звукового давления *P* можно записать: L_P (исх. 20 мкПа) = 20 дБ, а с использованием международных обозначений — L_P (re 20 μPa) = 20 dB (*re* — сокращение от англ. *reference*). Допускается указывать значение исходной величины в скобках за значением уровня, например: 20 дБ (исх. 20 мкПа). Также используется краткая форма, например, уровень L_W мощности *W* можно записать: L_W (1 мВт) = 30 дБ, илиL_W = 30 дБ (1 мВт). Значение «1» исходной величины может быть опущено, например, L_W = 30 дБ (мВт). То есть, если в скобках указана только размерность исходной величины, а значение величины не указано, то подразумевается, что оно равно «1». Для сокращения записи широко используются специальные обозначения, например: L_W = 30 дБм. Запись означает, что уровень мощности составляет +30 дБ относительно 1 мВт, то есть мощность равна 1 Вт.

Ниже приведены некоторые специальные обозначения, которые в предельно краткой форме указывают на значение исходной (опорной) величины, по отношению к которой определён соответствующий уровень, выраженный в децибелах [10;11]. Для указанных ниже опорных величин под электрическим напряжением понимается его среднеквадратичное (эффективное) значение.

- **dBW** (русское **дБВт**) — опорная мощность 1 Вт. Например, уровень мощности +30 дБВт соответствует мощности 1 кВт.
- **dBm** (русское **дБм**) — опорная мощность 1 мВт.
- **dBm0** (русское **дБм0**) — опорная мощность 1 мВт. Обозначение применяется в электросвязи для указания абсолютного уровня мощности, приведённого к так называемой точке нулевого относительного уровня.
- **dBV** (русское **дБВ**) — опорное напряжение 1 В.
- **dBuV** или **dBμV** (русское **дБмкВ**) — опорное напряжение 1 мкВ.
- **dBu** (русское **дБн**) — опорное напряжение ≈ 0,775 В, соответствующее мощности 1 мВт на нагрузке 600 Ом.
- **dBrn** — опорное напряжение соответствует мощности теплового шума идеального резистора с сопротивлением равным 50 Ом при комнатной температуре в полосе частот 1 Гц: Это значение соответствует уровню напряжения −61 dBμV или уровню мощности −168 dBm.
- **dB SPL** (от англ. *sound pressure level* — «уровень звукового давления») — опорное значение амплитуды звукового давления 20 мкПа, соответствующее порогу слышимости гармонического звукового колебания с частотой 1 кГц.
- **dB(A)**, **dB(B)**, **dB(C)** — эти символы применяются для обозначения взвешенного уровня звукового давления относительно 20 мкПа, когда при измерениях используются фильтры с соответствующими стандартными частотными характеристиками.
- **dBc** (русское **дБн**) — опорная величина соответствует мощности излучения на частоте несущей (англ. *carrier*).

- **dBi** (русское **дБи**) — изотропный децибел. Обозначение применяется для описания характеристик антенны (коэффициент направленного действия, коэффициент усиления) по сравнению с гипотетической изотропной антенной, которая равномерно излучает энергию по всем направлениям.
- **dBd** (русское **дБд**) — децибел относительно полуволнового вибратора (диполя). Обозначение применяется для описания характеристик антенны по сравнению с полуволновым вибратором (0 dBd = 2,15 dBi).
- **dBsm** (от англ. *square meter*, русское **дБкв.м** или **дБ(м²)**) — децибел относительно одного квадратного метра. Характеризует эффективную поверхность рассеяния рассеивателя в радиолокации.

По аналогии образуются составные единицы, например уровня спектральной плотности мощности: дБВт/Гц — «децибельный» аналог единицы Вт/Гц (мощность на номинальной нагрузке в полосе частот 1 Гц с центром на заданной частоте) — здесь опорный уровень 1 Вт/Гц.

В принципе за «нулевой уровень» можно принять любую величину. Так, например, "дБмкВ" (напряжение - отношение к одному микровольту), "дБВт" (мощность - отношение к одному ватту). В акустике за нулевой уровень звука принято звуковое давление $2 \cdot 10^{-5}$ Па - порог слышимости. При этом прямо так и измеряют уровень звука в децибелах [10;11]. Так сложилось исторически, потому что децибелы впервые применялись именно в области акустики. Но надо иметь ввиду - это как бы не «чистые» относительные децибелы, а «звуковые» - абсолютные. Например, шум реактивного самолета с расстояния 25 м равен 140 дБ, а 0 дБ - это порог слышимости. Часто можно встретить единицу под именем **dBA**. Она специально придумана для измерений интенсивности шумов. Величина дБА - уровень звукового давления, измеренный в "звуковых" децибелах при помощи шумомера, содержащего корректирующую цепочку, имитирующую чувствительность человеческого уха, что дает возможность получать отсчеты более соответствующие реальной слышимости шума. В технике проводной связи используют другую единицу - Непер. Неперы определяются не через десятичный, а через натуральный логарифм. При расчетах все эти **dB, dBi, dBm** по сути своей все являются децибелами, т.е. суммируются (если усиление) или вычитаются (если затухание), но **dBm** имеет приоритет как мера мощности сигнала. Например: Уровень на входе приемника (dBm) = Мощность передатчика (dBm) + Усиление антенн (dBi) - Ослабление сигнала (dB).

Технические характеристики и термины антенно-фидерных устройств

К АФУ относятся [10;11]: 1) антенны приемные; 2) антенны передающие; 3) антенны приемопередающие; 4)многовходовые антенные решетки; 5) многолучевые антенные решетки; 6) делители (распределители) мощности; 7) дуплексеры; 8) коммутаторы антенные передающие; 9)коммутаторы антенные приемные; 10) нагрузки; 11) ответвители направленные; 12)переключатели антенные; 13) устройства сложения сигналов; 14) устройства согласующие; 15) трансформаторы сопротивлений; 16) устройства симметрирующие; 17) фильтры; 18) фидеры. Классификации антенн по [10;11] представлена на рис.23.

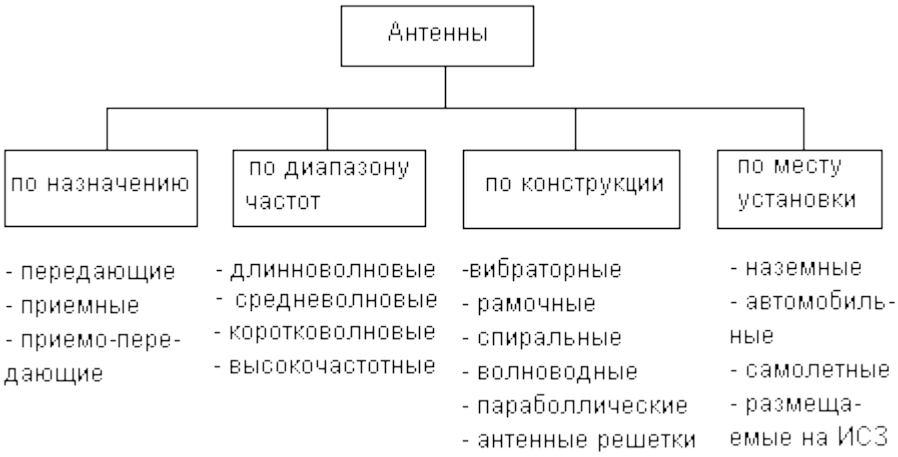


Рис.23. Классификации антенн

Основные типы антенн:

- Вибраторная антенна (Симметричный вибратор (диполь); Несимметричный вибратор);
- Антенна Ground Plane;
- Укороченная штыревая антенна;
- Колинеарная антенна;
- "Коаксиальная" антенна;
- J-образная антенна;
- Антенна зенитного излучения;
- Вертикальная антенна верхнего питания (Шунтовой вибратор; Петлевой вибратор ("Петлевой вибратор Пистолькорса"); Широкополосный "Диполь Наденeнко"; Турникетная антенна; Директорная антенна);
- Волновой канал (антенна Уда-Яги) (Антенна СГ (синфазная горизонтальная));
- Щелевая антенна (Щелевой вибратор; Волноводно-щелевая антенна);
- Апертурная антенна - антенна, излучение у которой происходит через раскрыв (плоское отверстие - апертуру).
- Используются в СВЧ-диапазоне.
- Рупорная антенна; Зеркальная антенна; Прямофокусная зеркальная антенна; Офсетная зеркальная антенна; Антенна Кассегрена; Антенна Грегори; Зеркальная антенна с косекансной диаграммой направленности; Зонтичная антенна; Рупорно-параболические антенны; Перископическая антенна; Линзовая антенна;
- Антенна с синтезированной апертурой;
- Антенна бегущей волны (Спиральная антенна; Диэлектрическая стержневая антенна; Импедансные антенны; Антенна вытекающей волны; Антенна Бевереджа; V-образная антенна; Ромбическая антенна; Антенна БС);
- Микрополосковая антенна; Патч-антенны; Сингулярная антенна;
- Чип-антенна (антненна, монтируемая по технологии SMD);
- Антенны оптического диапазона

- Наноантенна; Сверхширокополосные антенны; Антенна на принципе электродинамического подобия; Дискоконусная антенна;
- Излучатель типа "бабочка"; Логопериодическая антенна (Логарифмическая периодическая антенна); Фрактальная антенна; Т-рупор; Антенна Вивальди;
- Антенная решетка (система излучения) ;Фазированная антенная решётка;Пассивные ФАР
- Активные ФАР - с нелинейными преобразованиями сигнала в полотне решётки;
- Цифровая антенная решётка - активная ФАР с применением алгоритмов цифровой обработки сигнала непосредственно в полотне;
- MIMO-антенна; Антенны с линейными размерами << λ; Магнитная антенна; CFA-антенна;
- EH-антенна;
- Распределённые антенны; Частично излучающий кабель (коаксиальный кабель с намеренно ухудшенной экранировкой);
- Антенны для преобразования энергии электромагнитной волны в электрическую энергию и для средств RFID; Ректенна - антенна + выпрямитель;
- Наноантенна - антенна для резонансного преобразования излучения оптического диапазона в электрическую энергию

Антенны представляют собой конструкцию из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования радиосигналов в электрические. Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн. Назначение передающих и приемных антенны ясно из их наименований. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящихся под более высоким напряжением.

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

Характеристики антенн

1. ***Входное сопротивление антенны*** $z_{вх}$ является в общем случае комплексным, т.е. может быть представлено в виде последовательно соединенных активной $R_{вх}$ и реактивной $X_{вх}$ (емкостной или индуктивной) составляющих. Входное сопротивление настроенной в резонанс антенны чисто активно. ***Характеристика направленности*** - зависимость ЭДС в антенне либо мощности в нагрузке от угла прихода сигнала [10;11].

2. ***Диаграмма направленности*** - графическое изображение характеристики направленности в полярных или прямоугольных координатах (рис.24). Достаточно полное представление о направленных свойствах антенны дают диаграммы направленности в двух взаимно перпендикулярных плоскостях - горизонтальной и вертикальной.

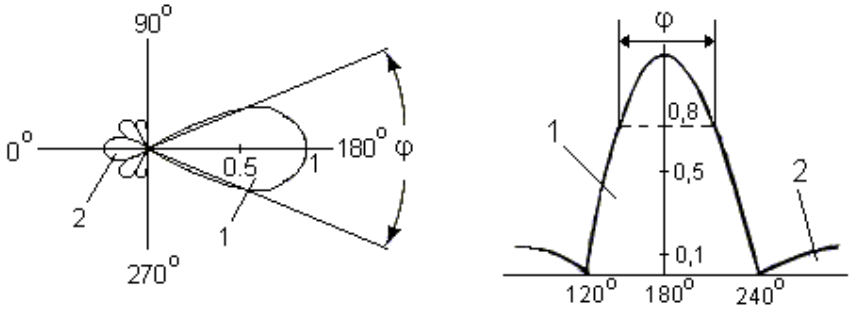


Рис.24. Диаграмма направленности антенн (область 1 - основной (главный) лепесток; область 2 - задний или боковой лепестки j- угол раствора основного лепестка)

При построении диаграмм направленности максимальное значение ЭДС в антенне или мощности в нагрузке принимают равным 1 или 0 дБ, что дает возможность сравнивать различные антенны по их направленным свойствам. Такие диаграммы направленности называют нормированными [10;11]. Чем меньше угол раствора главного лепестка и уровень задних и боковых лепестков, тем больше уровень сигнала на выходе антенны и выше помехозащищенность приема.

3. ***Коэффициент направленного действия (КНД).*** G - параметр, показывающий во сколько раз мощность, которую может отдать в нагрузку согласованная антенна при приеме со стороны максимума главного лепестка диаграммы направленности, больше мощности, которую может отдать в нагрузку эталонная антенна, имеющая круговую диаграмму направленности (рис.25). В качестве эталонной антенны служат простейшие антенны либо полуволновой вибратор.

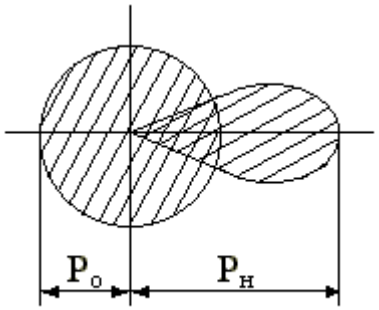


Рис 25. Коэффициент направленного действия антенны

В общем случае $G = P_н/P_о$, где $P_о$ - мощность при равномерном излучении в пределах от 0 до 360 градусов, $P_н$ - мощность при излучении в данном направлении.

4. ***Эффективная поверхность.*** $S_а$ - параметр, имеющий размерность площади и позволяющий по известной напряженности поля определить мощность Р, отдаваемую согласованной антенной в нагрузку: $P = \frac{E^2 S_a}{120\pi}$, где Р, Вт; Е - эффективное значение, В/м; $S_а$, м^2. $S_a = \frac{\lambda^2 G}{4\pi}$, где λ- длина волны излучаемого/принимаемого сигнала. В приемной антенне $S_а$ характеризует ЭДС сигнала, наводимую в антенне принимаемым электромагнитным излучением [10;11].

5. ***Диапазонность антенны.*** Антенна является резонансным устройством, и все ее характеристики зависят от частоты принимаемого/излучаемого сигнала (рис.26).

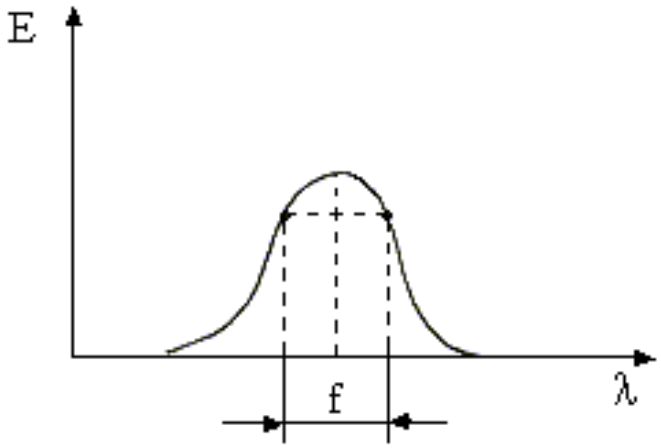


Рис.26. Частотные свойства антенны (E - ЭДС антенны λ - длина волны излучаемого/принимаемого сигнала f - частота резонанса (лучшее принятие сигнала)

Поляризация антенны - преимущественное направление изменения вектора электрического поля *E*. Поляризация бывает: горизонтальная, вертикальная, круговая и др. Например, антенны в виде металлических штырей или проводов имеют направление поляризации, направленное вдоль излучателей. Типичным представителем такой антенны является полуволновый вибратор [10;11]. Круговая поляризация может создаваться спиральной антенной, у которой излучатель свернут в виде спирали. Для эффективного приема сигнала приемная антенна должна располагаться так, чтобы ее плоскость поляризации совпадала с плоскостью поляризации передающей антенны. В противном случае сигнал будет очень слабым и будет формироваться за счет отражения от местных предметов (зданий, металлических конструкций), или приема не будет вовсе. Согласование антенны с кабелем характеризуется **коэффициентом бегущей волны** (КБВ) [10;11]. При отсутствии идеального согласования антенны и кабеля имеет место отражение падающей волны, например, от конца кабеля или другой точки, где его свойства резко меняются. В этом случае вдоль кабеля распространяются в противоположных направлениях падающая и отраженная волны. В тех точках где фазы обеих волн совпадают, суммарное напряжение максимально, а в точках, где фазы противоположны, оно минимально. В идеальном случае КБВ = 1 (когда имеет место режим бегущей волны, то есть ко входу телевизора передается сигнал максимально возможной мощности, так как в кабеле нет отраженных волн). Это возможно при согласовании входных сопротивлений антенны, кабеля и телевизора. В наихудшем случае КБВ = *0* (имеет место режим стоячей волны, то есть амплитуды падающей и отраженной волн равны, и энергия вдоль кабеля не передается).

Коэффициент стоячей волны определяется соотношением: КСВ=1/КБВ. Реальный выигрыш антенны по мощности относительно гипотетического изотропного

излучателя или полуволнового вибратора характеризуется **коэффициентом усиления по мощности** *Кр*, который связан с КНД соотношением $K_P = D\eta$, где -η **коэффициент полезного действия** (КПД) антенны. КПД антенны характеризует потери мощности в антенне и представляет собой отношение мощности излучения к сумме мощностей излучения и потерь, то есть к полной мощности, которая подводится к антенне от передатчика: $\eta = \frac{P_U}{P_U+P_n} = \frac{R_U}{R_U+R_n}$, где Pu - мощность излучения, Pn - мощность потерь, Ru - сопротивление излучения, Rn - сопротивление потерь.

Принципы использования антенн для одновременной передачи и приема

Необходимым условием одновременного использования одной антенны для приема и передачи является разнос частот приема и передачи, однако обе частоты должны лежать в полосе частот, принимаемых антенной [10;11]. При таком использовании антенны возникают два неприятных явления: 1. Мощный выходной сигнал передатчика проникает на входные высокочувствительные цепи приемника и выводит их из строя; 2. Слабый сигнал ЭДС, наводимый принимаемым антенной электромагнитным излучением, шунтируется выходными цепями передатчика и ослабляется, что препятствует нормальному приему сигнала. Для исключения этих явлений производится развязка входных и выходных цепей [10;11] с помощью фильтров-пробок (т.е. не пропускающих сигнал определенной частоты), включаемых в соответствующие цепи приемопередатчика, так, как показано на рис.27.

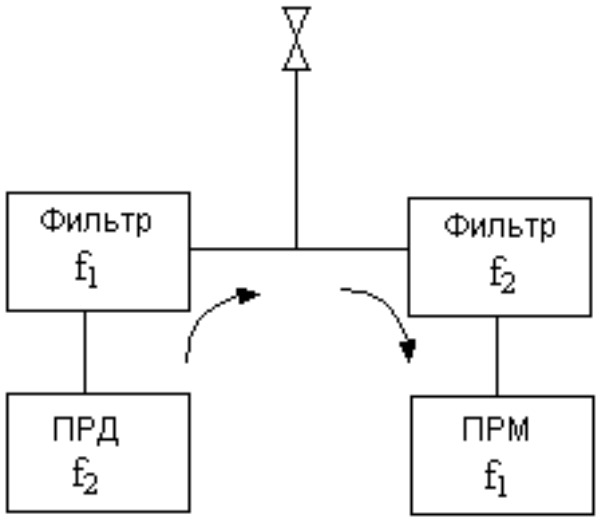


Рис.27. Развязка входных и выходных цепей с помощью фильтров-пробок

ПРД – передатчик ПРМ – приемник Передающие и приемные линии никогда не работают на одной частоте. Фильтр для частоты f_2 не пропускает частоту f_2 на входные цепи приемника, а фильтр для частоты f_1не пропускает сигнал с частотой f_1, поступающий из антенны, на выходные цепи передатчика.

3.5. Основные термины, определения и технические характеристики средств защиты информации в проводных линиях связи

Классификация утечек информации в проводных линиях связи

Для перехвата информации с различных типов кабелей используются разные типы устройств:

- для симметричных высокочастотных кабелей - устройства с индукционными датчиками;
- для коаксиальных высокочастотных кабелей - устройства непосредственного (гальванического) подключения;
- для низкочастотных кабелей - устройства непосредственного (гальванического) подключения, а также устройства с индукционными датчиками, подключаемыми к одному из проводов.

Телефонный канал утечки.

Подслушивание телефонных переговоров в рамках промышленного шпионажа возможно [8;28;15;31;33]:

1) Гальваническая съем телефонных переговоров (путем контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети) определяется путем ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры.

2) Телефонно-локационный способ (по телефонной линии передается высокочастотный тональный сигнал, который воздействует на нелинейный элемент телефонного аппарата (диоды, транзисторы, микросхемы) на который также воздействует акустический сигнал. В результате в телефонные линии формируются высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала (ADSL модемы). Трудность данного способа съема информации заключается в том что дальность такой системы из за затухания высоко частотного сигнала в двух проводной линии не превышает ста метров.

3) Индуктивный и емкостной способ негласного съема телефонных переговоров.

4) Индуктивный способ работает за счет электромагнитной индукции возникающей в процессе телефонных переговоров вдоль провода телефонной линии. качество приемного устройства съема информации использовать трансформатор. Первичная обмотка которого охватывает один или 2 провода телефонной линии.

5) Емкостной способ работает за счет формирование на обкладках конденсатора электростатического поля изменяющийся соответствующим изменением уровня телефонных переговоров. в качестве приемника используется емкостной датчик. выполненный в виде двух пластин плотно прилегающих к проводам телефонной линии. Классификация электронных устройств перехвата информации в проводных линиях связи [8;28;15;31;33] представлена в таблице 17. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники [8;28;15;31;33] представлена в таблице 18.

Таблица 17

Классификация электронных устройств перехвата информации в проводных линиях связи (телефонные закладки)

№ п/п	Показатель классификации	Значения
1	Вид датчика	1. телефонный адаптер; 2. магнитная антенна
2	Способ подключения к линии	1. последовательное (с разрывом одного провода); 2. параллельное (с разрывом или без разрыва двух проводов); 3. индуктивное
3	Место установки	1. в корпусе тлф. аппарату или трубке; 2. в телефонной розетке или коммутационных изделиях и на кроссе; 3. в телефонной линии
4	Способ передачи информации	1. по тлф. линии (занятой или не занятой); 2. по радиоканалу; 3. по сети электропитания; 4. по ИК-каналу
5	Тип источника питания	1. автономный источник; 2. от телефонной линии; 3. от сети 220В
6	Вид исполнения	1. обычный (модульный); 2. камуфлированный
7	Способ управления передатчика	1. не управляемые; 2. с автопуском (акустоматы); 3. с дистанционным управлением; 4. автопуск по таймеру
8	Способ накопления информации	1. без накопления; 2. с накоплением (коротким и длительным накоплением)
9	Способ кодирования информации	1. без кодирования; 2. с аналоговым скремблированием; 3. с цифровым шифрованием
10	Используемый диапазон частот для передачи информации	- VHF очень высокочастотный (метровые волны); - UHF ультравысокочастотный (дециметровые волны); - SHF сверхвысокочастотный (сантиметровые волны).
11	Вид используемых сигналов	1. с простыми сигналами (АМ,ЧМ модуляция); 2. цифровые сигналы с частотной модуляцией 3. со сложными сигналами (ШПС, сл. фазой и пр.); 4. с псевдослучайной перестройкой частоты (ППРЧ)

Таблица 18

Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники

№ п/п	Показатель классификации	Значения
1	Вид перехватываемой информации	- видеоизображение с экрана монитора; - информация вводимая с клавиатуры; - информация выводимая на принтер; - информация, записываемая на жесткий диск; - информация, записываемая на внешние носители; - информация, передаваемая по каналам связи
2	Место установки	- в корпусе системного блока; - подключение к внешним разъемам системного блока; - подключение в виде переходных элементов (разъемов) соединительных кабелей с переферией; - в корпусе монитора; - в корпусе принтера; - в корпусе клавиатуры (мыши); - в корпусе другой периферии
3	Способ передачи информации	- без передачи информации (с записью на носитель); - по радиоканалу; - по сети питания; - по выделенной лини; - по оптическому каналу; - по ЛВС
4	Средство передачи информации	- специальная радиозакладка; - ИК порт; - устройства Bluetooth WI-FI, WIN MAX и пр.
5	Тип источника питания	- от сети 220В - от низковольтных источников питания технических средств; - автономное питание
6	Вид исполнения	- обычное (отдельные модули); - камуфлированное под устройства и элементы радиоэлектронных средств и устройства коммутации
7	Способ управления передатчика	- не управляемые; - с дистанционным управлением; - автопуск по таймеру
8	Способ накопления информации	- без накопления; - с накоплением (коротким и длительным накоплением)
9	Способ кодирования информации	- без кодирования; - с цифровым шифрованием

Защита оконечного оборудования слаботочных линий от от микрофонного эффекта и ВЧ-навязывания.

Пассивная защита осуществляется путем ограничения и фильтрации или отключением источников опасных сигналов [15;31;33]. В схемах ограничителей используют встречно включенные полупроводниковые диоды, сопротивление которых

для малых (преобразованных) сигналов, составляющее сотни килоом, препятствует их прохождению в слаботочную линию. Для токов большой амплитуды, соответствующих полезным сигналам, сопротивление оказывается равным сотням Ом и они свободно проходят в линию.

Фильтрация является средством борьбы с ВЧ-навязыванием [15;31;33]. Роль простейших фильтров выполняют конденсаторы, включаемые в микрофонную и звонковую цепи. Шунтируя высокочастотные сигналы навязывания, они не воздействуют на полезные сигналы. Для защиты телефонных аппаратов, как правило, используют приборы, сочетающие свойства фильтра и ограничителя [15;31;33]. Активная защита оконечных устройств осуществляется путем маскирования полезных сигналов. Например, изделия серии МП, снабженные фильтрами от ВЧ-навязывания, генерируют в линии шумоподобные колебания. Устройство МП-1 А (для аналоговых линий) реализует этот режим только при положенной телефонной трубке, а МП-1 Ц (для цифровых линий) — постоянно. Защиту трехпрограммных трансляционных приемников обеспечивают приборы МП-2 и МП-3, вторичных электрочасов — МП-4, динамиков оповещения — МП-5, который дополнительно гальванически отключает их от линии при отсутствии полезных сигналов.

Устройство типа «Телефонное ухо». Устройство «Телефонное УХО» предназначено для осуществления скрытного дистанционного акустического контроля помещения, в котором оно установлено [15;31;33]. Питается оно от телефонной линии. Прослушивание осуществляется по телефонной линии посредством звонка по специальному алгоритму с любого удалённого телефона. При этом устройство не мешает нормальной работе телефонов, подключенных к этой линии и работает незаметно для абонента, находящегося в контролируемом помещении (если абонент поднимает трубку, прослушивание автоматически прерывается).

Для исключения возможности использования «Телефонного УХА» посторонними лицами активизация режима прослушивания производится тоновым набором пароля из трёх цифр. Кроме того, тоновым набором задаётся номер подключенного микрофона. Если используемый для прослушивания телефонный аппарат не имеет возможности тонового набора, можно воспользоваться биппером.

«Телефонное УХО» смонтировано в обычной телефонной розетке и состоит из двух плат: основной и платы микрофона с усилителем. Чувствительность встроенного микрофона позволяет контролировать разговор на расстоянии 3...10 метров. Возможно дополнительное подключение до трёх аналогичных внешних микрофонов. Платы дополнительных микрофонов размещаются в удобных местах и соединяются с основной платой проводами. «Телефонное УХО» имеет массу преимуществ перед радиомикрофоном: практически неограниченный радиус действия, отсутствие радиоизлучения, и как следствие, невозможность обнаружения и прослушивания посторонними лицами. Для того чтобы активизировать режим прослушивания необходимо позвонить на объект специальным образом - двойным набором номера: сначала нужно позвонить и положить трубку после 2-го гудка, затем незамедлительно позвонить второй раз (допустимая задержка до 30 с). Если все сделано правильно, будут слышны короткие гудки, сигнализирующие о том, что система активизировалась. Далее, для перехода к прослушиванию помещения, необходимо тоновым набором с

телефона ввести специальный код. Если код не будет набран, короткие гудки продлятся в течение 80 с, после чего включится режим прослушивания. Максимальное время прослушивания составляет 60 минут. Режим прослушивания автоматически выключается при поднятии трубки телефона на контролируемом объекте или опускании телефонной трубки на телефоне, с которого ведётся прослушивание. Устройство автоматически блокирует прохождение на объект первых двух звонков, поэтому при включении прослушивания телефоны на объекте не звонят, что обеспечивает скрытность работы системы прослушивания.

Линейное зашумление. Системы линейного зашумления применяются для маскировки опасных сигналов в проводах, кабелях, различных токоведущих линиях и конструкциях, выходящих за пределы контролируемой территории [15;31;33]. Объектами линейного зашумления являются, например, провода, цепи и устройства технических средств, подверженные воздействию низкочастотных электромагнитных полей, возникающих при работе ТСОИ, а также элементы и устройства, обладающие свойствами электроакустических преобразователей.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который подключается в зашумляемую токоведущую линию.

Основные способы защиты телефонных линий. Защита телефонных разговоров от перехвата осуществляется главным образом активными методами [15;31;33]. К основным из них относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления");
- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод "выжигания").

Суть **метода синфазной маскирующей низкочастотной (НЧ) помехи** заключается в подаче в каждый провод телефонной линии с использованием единой

системы заземления аппаратуры АТС и нулевого провода электросети 220 В (нулевой провод электросети заземлен) согласованных по амплитуде и фазе маскирующих сигналов речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (телефонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значительно превосходит полезный сигнал, то перехват информации (выделение полезного сигнала) становится невозможным. В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности импульсов).

Метод синфазного маскирующего низкочастотного сигнала используется для подавления телефонных радиозакладок (как с параметрической, так и с кварцевой стабилизацией частоты) с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) с помощью индукционных датчиков различного типа.

Метод **высокочастотной маскирующей помехи** заключается в подаче во время разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового диапазона. Данный метод используется для подавления практически всех типов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индукционных датчиков. Однако эффективность подавления средств съема информации с подключением к линии при помощи с индукционных датчиков (особенно не имеющих предусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа "белого шума" или дискретные сигналы типа псевдослучайной последовательности импульсов. Частоты маскирующих сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора закладки или микрофонного усилителя диктофона их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал. Обычно используются частоты в диапазоне от 6 ... 8 кГц до 16 ... 20 кГц. Например, в устройстве Sel SP-17/T помеха создается в диапазоне 8 ... 10 кГц.

Такие маскирующие помехи вызывают значительные уменьшение отношения сигнал/шум и искажения полезных сигналов (ухудшение разборчивости речи) при перехвате их всеми типами подслушивающих устройств. Кроме того, у радиозакладок с параметрической стабилизацией частоты ("мягким" каналом) как последовательного, так и параллельного включения наблюдается "уход" несущей частоты, что может привести к потере канала приема.

Для исключения воздействия маскирующего помехового сигнала на телефонный

разговор в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов. Аналогичную роль выполняют полосовые фильтры, установленные на городских АТС, пропускающие сигналы, частоты которых соответствуют стандартному телефонному каналу (300 Гц ... 3,4 кГц), и подавляющие помеховый сигнал.

Метод **ультразвуковой маскирующей помехи** в основном аналогичен рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20 ...25 кГц до 50... 100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиозакладок. Поднятие напряжения в линии до 18 ... 24 В вызывает у радиозакладок с последовательным подключением и параметрической стабилизацией частоты "уход" несущей частоты и ухудшение разборчивости речи вследствие размытия спектра сигнала. У радиозакладок с последовательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3 ... 10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод "обнуления" предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности. Этот метод используется для нарушения функционирования подслушивающих устройств с контактным параллельным подключением к линии и использующих ее в качестве источника питания. К таким устройствам относятся: параллельные телефонные аппараты, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, акустические и телефонные закладки с питанием от телефонной линии и т.д.

Метод низкочастотной маскирующей помехи заключается в подаче в линию при положенной телефонной трубке маскирующего сигнала (наиболее часто, типа "белого шума") речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц) и применяется для подавления проводных микрофонных систем, использующих телефонную линию для передачи информации на низкой частоте, а также для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (то есть при отсутствии полезного сигнала).

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии.

Суть метода заключается в следующем. При передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого

диапазона с известным спектром). Одновременно этот же маскирующий сигнал ("чистый" шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи. Недостатком данного метода является то, что маскировка речевых сообщений односторонняя и не позволяет вести двухсторонние телефонные разговоры.

Метод "выжигания" реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

Методы контроля телефонных линий в основном основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии [15;31;33].

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряжение, соответствующее нормальному состоянию линии (когда к линии не подключены посторонние устройства), и порог тревоги. При уменьшении напряжения в линии более установленного порога устройством подается световой или звуковой сигнал тревоги.

На принципах измерения напряжения в линии построены и устройства, сигнализирующие о размыкании телефонной линии, которое возникает при последовательном подключении закладного устройства. Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет "микрофонного эффекта" в элементах телефонного аппарата и высокочастотного "навязывания". Устройства контроля телефонных линий, построенные на рассмотренном принципе, реагируют на изменения напряжения, вызванные не только подключением к линии средств съема информации, но и колебаниями напряжения на АТС (что для отечественных линий довольно частое явление), что приводит к частым ложным срабатываниям сигнализирующих устройств. Кроме того, эти устройства не позволяют выявить параллельное подключение к линии высокоомных (с сопротивлением в несколько МОм) подслушивающих устройств. Поэтому подобные устройства не находят широкого применения на практике.

Принцип работы более сложных устройств основан на периодическом измерении и анализе нескольких параметров линии (наиболее часто: напряжения, тока, а также комплексного (активного и реактивного) сопротивления линии). Такие устройства позволяют определить не только факт подключения к линии средств съема информации, но и способ подключения (последовательное или параллельное).

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съема

информации, оборудованы и средствами их подавления [15;31;33]. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

Для блокировки работы (набора номера) несанкционированно подключенных параллельных телефонных аппаратов используются специальные электронные блокираторы [15;31;33].

Принцип работы подобных устройств состоит в следующем. В дежурном режиме устройство защиты производит анализ состояния телефонной линии путем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппарате снята), срабатывает звуковая и световая (загорается светодиод несанкционированного подключения к линии) сигнализация. А если факт несанкционированного подключения к линии зафиксирован в отсутствии телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнализация и устройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата.

В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя снятие трубки на защищаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата. Кроме несанкционированного подключения к линии параллельного телефонного аппарата подобные устройства сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.

Весьма эффективной мерой противодействия подслушиванию переговоров является использование для ведения конфиденциального общения ***маскираторов речи или скремблеров*** [15;31;33]. На сегодня техника шифрования речевых сигналов достаточно развита и появилась на рынке в виде удобных переносных или стационарных аппаратов, надежно шифрующих речевой сигнал до его подачи в телефонную линию.

Скремблер - это автономное или встроенное устройство для засекречивания речевой информации, передаваемой по каналам проводной и радиосвязи.

Выбор той или иной модели скремблера зависит от его конкретного применения и характеристик канала связи. Модели скремблеров, предлагающиеся на отечественном рынке, различаются назначением, конструктивным исполнением и возможностями, а также стойкостью засекречивания, порядком ввода ключа, качеством восстановленной речи, способом электропитания, конструкцией (встроенный или автономный) и другими характеристиками [2815;31;33]. В таблице 19 приведены некоторые типы отечественных и зарубежных скремблеров.

Таблица 19

Характеристики некоторых скремблеров

№ п/п	Тип	Конструкция	Основные особенности
1	SCR- M12	Крипто-телефонная	Защита телефонов и факсов приставка
2	СТА-1000	Приставка к телефонному аппарату	Защита телефонных переговоров по сетям общего пользования
3	"Орех"	Телефонная приставка	
4	ASC-2	Автономное кодирующее устройство.	Может использоваться с любыми аппаратами: таксофоны, радиотелефоны, сотовая связь и др. Защищает как от прямого подслушивания, так и от закладных устройств в телефонных аппаратах
5	"Разбег-К"	Абонентский телефонный маскиратор	Защита телефонных переговоров. Имеет стаж RS-232. Защищен от микрофонного эффекта и ВЧ-навязывания
6	"Уэа"	Телефонный маскиратор	Размещен в чемодане типа кейс. Подключа ется к линии напрямую или через акустический соединитель. Возможен разговор с таксофона
7	Р-117Л	Скремблер	Защита переговоров, ведущихся по радиоканалам. Совместим с большинством портативных радиостанции
8	"Туман"	Маскиратор	Предназначен для маскирования телефон ных переговоров по абонентским линиям связи. Аппарат включается в разрыв проводов, идущих от телефонного аппарата к микротелефонной трубке
9	"Селена"	Маскиратор	Малые габариты и простота подключения к любым телефонным линиям позволяют брать его в деловые поездки
10	Е-24	Аппаратура закрытия речевой информации	Используется с радиостанциями Р-159
11	Е-9к	Аппаратура закрытия речевой и цифровой информации	"
12	АТ-2400	Аппаратура ведения конфиденциальных телефонных переговоров	Выполнен в виде приставки к телефонному аппарату
13	"Voice changer"	Изменитель голоса	Предназначен для изменения голоса при телефонном разговоре. Позволяет в широких пределах изменять тембр голоса и делает речь полностью неузнаваемой
14	Линия-1	Устройство конфиденциальной связи	Предназначено для защиты речевой информации в линиях телефонной связи. Используется метод инверсии спектра

Характеристики оборудования защиты в проводных линиях связи

Аппаратура проверки проводных линий.

По своему назначению и конструктивному исполнению аппаратура проверки проводных линий может быть ***оперативной и профессиональной***.

К оперативным средствам можно отнести, например, анализатор телефонной линии "АТЛ-1" (МПО "Защита информации") [15;31;33]. Этот анализатор предназначен для защиты телефонной линии от несанкционированного подключения в нее любых устройств с сопротивлением до 5 кОм.

При подключении прибора к телефонной линии линия считается "чистой" и под такую линию прибор настраивается в режим контроля. При несанкционированном подключении к линии загорается красный индикатор (режим обнаружения). При нормальной работе линии горит зеленый индикатор.

Используются и более сложные профессиональные комплексы [15;31;33]. Такие, например, как тест-комплект для проверки проводных линий. Такой тест-комплект предназначен для выявления гальванических подключений к любой проводной линии: телеграфной и телефонной связи, звукозаписи и воспроизведения и др.; переговорных устройств, систем звукоусиления; трансляции, сигнализации и др. В комплект входят: анализатор, тестер, соединительные провода со щупами, съемные зажимы типа "крокодил", защитное устройство, кейс.

Характеристики:

- максимальная величина тока нагрузки при напряжении зондирующего сигнала 150 В - 1 ма;
- частота зондирующего сигнала - 40 и 400 Гц;
- дальность зондирования - 5000 м.

Зарубежные анализаторы телефонных линий представляют фирмы DYNATEL. Анализатор типа 965 MC представляет собой переносное устройство с микропроцессорным управлением, предназначенное для измерений, диагностики и определения мест повреждений проводников в телефонных кабелях.

Анализатор обеспечивает возможность определения: величины напряжения; омического сопротивления обрывов - до 100 Мом; мест понижения сопротивления изоляции - до 30 Мом; величины тока; затухания; шума; тонального сигнала; а также обнаруживает устройства, которые регулируют напряжение или ток в линии; обеспечивает контроль за абонентской линией, набирает телефонный номер, хранящийся в памяти, и предусматривает ручной набор; выбирает тип батареи, режим заряда батареи, опознавание владельца; производит преобразование величин сопротивлений, выраженных в омах, в эквивалентную длину, выраженную в метрах, а также преобразует длину, выраженную в метрах, в величину сопротивления, выраженную в омах.

Обнаружив факт несанкционированного подключения, необходимо установить, где оно осуществлено. Место контактного подключения определяется импульсным методом с помощью импульсных приборов. Импульсный метод основан на использовании явления отражения электромагнитных волн от места подключения к линии подслушивающего устройства. Зная скорость распространения электромагнитной энергии V и время t с момента посылки импульса и возврата его обратно, определяют расстояние до места подключения: $L = Vt/2$.

Если подключение осуществлено в пределах контролируемой зоны или территории, то используются организационные меры противодействия: изъятие подключенного устройства и защита коммуникаций физическими средствами и мерами. Если же подключение осуществлено за пределами контролируемой территории, следует принять определенные действия по защите информации: не вести конфиденциальные переговоры по этой телефонной линии; установить маскиратор речи.

Имеются средства более радикальной борьбы, например электрическое уничтожение (прожигание) подслушивающих устройств, установленных в телефонную линию на участке от АТС до абонентского телефонного аппарата [15;31;33]. К числу таких устройств относится, например, генератор импульсов КС-1300. Это устройство работает в ручном и автоматическом режиме. В ручном режиме пользователю дается право выбора момента подачи в телефонную линию сигнала уничтожения подслушивающего устройства. В автоматическом режиме прожигающий импульс посылается в линию по регламенту с определенной частотой. Устройство обладает следующими техническими характеристиками:

- количество подключаемых телефонных линий - 2;
- временные интервалы, устанавливаемые таймером, - от 10 минут до 2 суток;
- мощность прожигающего импульса - 15 Вт;
- потребляемая мощность - 40 Вт;
- питание - сеть 220 В.

В качестве мер защиты внутренних коммуникаций от незаконного подключения необходимо: экранирование всех коммуникаций, по которым ведутся конфиденциальные переговоры; установка средств контроля мест возможного доступа к линиям связи; использование телефонных систем внутреннего пользования без их выхода в город и другие меры.

Противодействие бесконтактному подключению. Бесконтактный (индуктивный) съем информации осуществляется путем прикосновения бесконтактного датчика к телефонной линии и прослушивания переговоров на головные телефоны или их записи на магнитофон [15;31;33]. Индукционный контакт датчика с телефонной линией не вносит никаких изменений в параметры телефонной

линии, что весьма ограничивает возможности по обнаружению такого контакта техническими средствами, особенно в том случае, если телефонная линия не подвергается физическим воздействиям. Если же попытка подключения совершается по отношению к экранированным телефонным линиям, то есть определенные возможности обнаружить бесконтактное подключение приборными средствами. При бесконтактном подключении к экранированным кабелям частично снимается экранирующая оплетка. Этого уже достаточно, чтобы обнаружить повреждение экранного покрытия. Точное определение места повреждения экрана определяется импульсным методом точно так, как это делалось при контактном подключении [15;31;33]. Более точно место повреждения определяется подачей в линию звуковых частот и их приемом при движении по трассе кабеля специальным поисковым прибором.

Этот специальный поисковый прибор предназначен для точного определения места повреждения кабелей связи. Прибор работает совместно с генератором звуковых частот, работающим на частотах 1,03 кГц и 10 кГц. Мощность сигнала генератора звука при работе от встроенных батарей составляет 3 Вт, а при питании от внешней батареи или от сети - 10 Вт. Поиск места повреждения осуществляется проходом по трассе кабеля и определением места излучения звуковой частоты, посылаемой в линию звуковым генератором.

Противодействие бесконтактному подключению осуществляется также организационными и организационно-техническими мерами [15;31;33]. В качестве последних рекомендуется использовать генераторы шума и специальные защитные модули. К таким можно отнести универсальный телефонный защитный модуль, способный подавлять индуктивные съемники, микропередатчики, блокировать атозапуск диктофонов. Кроме того, отдельные образцы таких модулей обеспечивают контроль малейших изменений, производимых в телефонных линиях. Не исключается и посылка прожигающего импульса в линию предполагаемого бесконтактного съема информации.

3.6. Основные термины, определения и технические характеристики средств защиты информации по каналам мобильной связи, Bluetooth и WI-FI

Угрозы передаваемой информации в сетях сотовой связи. В сетях сотовой связи происходит реализации следующих действий злоумышленниками [34;1;35;36;37]:
– массовая рассылка рекламной или иной информации, не запрашиваемой пользователями сети сотовой связи, адресованная на серверы соответствующих служб оператора связи или на абонентские терминалы, с использованием средств самого оператора или Интернета;
– клонирование модулей SIM;

– хакерский взлом систем автоматизированного расчета с абонентами (биллинга);
– мошенничество с картами предоплаты.

Стандарты мобильной связи. Поколения мобильной телефонии [34;1;35;36;37] представлена в таблице 20.

Таблица 20

Поколения мобильной телефонии

Поколение	1G	2G	2.5G	3G	3.5G	4G
Начало разработок	1970	1980	1985	1990	до 2000	с 2000
Реализация	1984	1991	1999	2002	2006-2007	2008-2010
Сервисы	аналоговый стандарт, синхронная передача данных со скоростью до 9,6 кбит/с	цифровой стандарт, поддержка коротких сообщений (sms)	большая емкость, пакетная передача данных	еще большая емкость, большие скорости	увеличение скорости сетей третьего поколе- ния	большая емкость, IP-ориентированная сеть, поддержка мультимедиа, скорости до сотен Мбит/с
Ширина канала	1,9 кбит/с	14,4 кбит/с	384 кбит/с	2 Мбит/с	3-14 Мбит/с	1 Гбит/с
Стандарты	AMPS, TACS, NMT	TDMA, CDMA, CDMA One, GSM, PDC, DAMPS	GPRS, EDGE, 1xRTT	WCDMA, CDMA 2000, UMTS	HSDPA	единый стандарт
Сеть	PSTN	PSTN	PSTN, сеть пакетной передачи данных	сеть пакетной передачи данных	сеть пакетной передачи данных	Интернет

Методы обеспечения безопасности в сетях GSM (A3, A5, A8). Действующие нормативные документы организации разработчиков стандарта GSM определяют, что системы сотовой связи (ССС) этого стандарта должны обеспечивать следующие механизмы защиты системных и информационных ресурсов [34;1;35;36;37]:

–защита от несанкционированного доступа к мобильной станции (МС) с помощью парольного метода защиты;

–идентификация мобильного абонента ССС с помощью его уникального международного идентификационного номера (МИН);

–аутентификация (определение подлинности) абонента при каждом вхождении в связь с помощью алгоритма А3;

–конфиденциальность передаваемой по радиоканалу информации путём её шифрования с помощью алгоритма А5, где ключ шифрования вычисляется алгоритмом А8;

–секретность местонахождения абонента и направления его вызова.

Криптографическая защита информационных ресурсов систем сотовой связи обеспечивается за счет использования алгоритмов А3, А5 и А8, носителем которых, за исключением А5, является SIM-карта абонента.Криптозащита сотовой связи стандарта GSM обеспечивается тремя секретными алгоритмами:

А3 - алгоритм, используемый при аутентификации пользователя, он же защищает его от клонирования;

А5 - алгоритм шифрования голосового трафика, который и обеспечивает защиту телефонных переговоров; до недавнего времени в мире существовало две его версии: А5/1 - усиленный алгоритм, используемый в некоторых странах, А5/2 - его ослабленный аналог;

А8 - алгоритм генерации ключа, который берет результат работы А3 и превращает его в сеансовый ключ А5; алгоритм А5, отвечающий за защиту переговоров от перехвата, реализован на аппаратном уровне в мобильных телефонах и базовых станциях.

АЛГОРИТМ А8. Схема аутентификации на шифре А8 для сетей GSM представлена на рис.28 [34;1;35;36;37]. Для исключения несанкционированного использования ресурсов системы связи вводятся механизмы аутентификации. У каждого подвижного абонента есть стандартный модуль подлинности абонента (SIM-карта), которая содержит:

- международный идентификационный номер подвижного абонента (IMSI — International Mobile Subscriber Identity)
- свой индивидуальный 128-битный ключ аутентификации (Ki)
- алгоритм аутентификации (А3), и генерации сеансового ключа (А8).

Ключ аутентификации пользователя Ki уникален и однозначно связан с IMSI, оператор связи по значению IMSI «умеет» определять Ki и вычисляет ожидаемый результат. От несанкционированного использования SIM защищена вводом индивидуального идентификационного номера (PIN-код — Personal Identification Number), который присваивается пользователю вместе с самой картой. Рассмотрим процедуру проверки подлинности абонента. Сеть генерирует оказию — случайный номер (RAND) и передаёт его на мобильное устройство. В Sim-карте происходит вычисление значения отклика (SRES — Signed Response) и сеансового ключа, используя RAND, Ki и алгоритмы А3,А8. Мобильное устройство вычисляет SRES и посылает его в сеть, которая сверяет его с тем, что вычислила сама. Если оба значения совпадают, то аутентификация пройдена успешно и мобильное устройство получает от

сети команду войти в шифрованный режим работы. Из-за секретности все вычисления происходят внутри SIM. Секретная информация (такая как Ki) не поступает вне SIM-карты. Ключ Kc также не передаётся по радиоканалу. Подвижная станция (ПС) и базовая станция(БС) вычисляют их отдельно друг от друга.

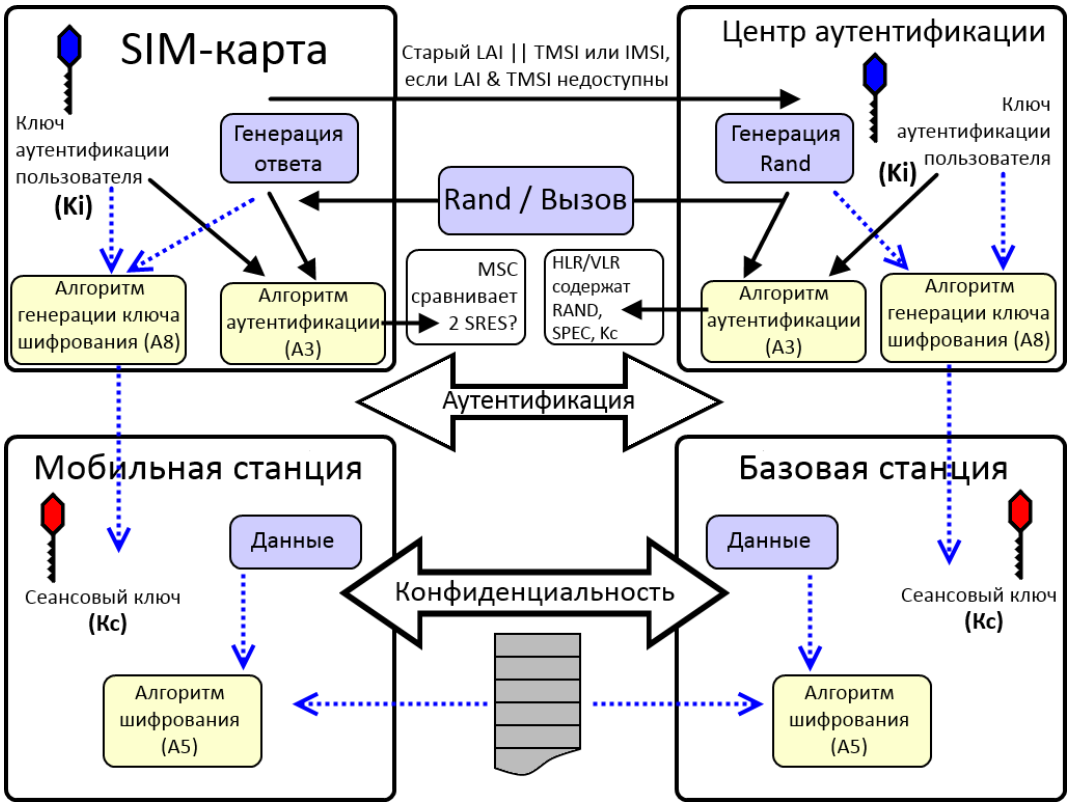


Рис.28 Схема аутентификации на шифре A8 для сетей GSM

Фактически алгоритмы A3 и A8 можно было бы реализовать в форме одного-единственного вычисления. Например, в виде единого алгоритма, выходные данные которого состоят из 96 бит: 32 бита для образования SRES и 64 бита для образования Kc. Следует отметить, что длина значимой части ключа Kc, выданная алгоритмом A8, устанавливается группой подписей GSM MoU и может быть меньше 64 бит. В этом случае значимые биты дополняются нулями для того, чтобы в этом формате всегда были использованы все 64 бита.

Всякий раз, когда какая-либо мобильная станция проходит процесс аутентификации, данная мобильная станция и сеть также вычисляют ключ шифрования Kc, используя алгоритм A8 с теми же самыми вводными данными RAND и Ki, которые используются для вычисления SRES посредством алгоритма A3.

Поточные шифры. Криптографические методы обеспечения безопасности можно разделить на две большие группы: блочные шифры и поточные [34;1;35;36;37]. Блочные обрабатывают поступающую информацию, предварительно разбивая ее на блоки определенной длины, как правило, вносят задержку и предназначены для закрытия данных. Поточные шифры обрабатывают информацию в реальном масштабе

времени, без разделения на блоки и наиболее подходят для закрытия речи.

ШИФР RC4. Это потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритме безопасности беспроводных сетей WEP, для шифрования паролей в Windows NT) [34;1;35;36;37]. Алгоритм RC4 строится как и любой потоковый шифр на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Длина ключа обычно составляет от 5 до 64 байт. Максимальная длина ключа 256 байт. Основные преимущества шифра — высокая скорость работы и переменный размер ключа. RC4 довольно уязвим, если используются не случайные или связанные ключи, один ключевой поток используется дважды. Эти факторы, а также способ использования могут сделать криптосистему небезопасной (например WEP).

Ядро алгоритма состоит из функции генерации ключевого потока. Эта функция генерирует последовательность битов (ki), которая затем объединяется с открытым текстом (mi) посредством суммирования по модулю два. Так получается шифрограмма (ci): $c_i = m_i \oplus k_i$. Расшифровка заключается в регенерации этого ключевого потока (ki) и сложении его и шифрограммы (ci) по модулю два. В силу свойств суммирования по модулю два на выходе мы получим исходный незашифрованный текст (mi): $m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$. Другая главная часть алгоритма – функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока. RC4 – фактически класс алгоритмов, определяемых размером его блока. Этот параметр n является размером слова для алгоритма. Обычно, n = 8, но в целях анализа можно уменьшить его. Однако для повышения безопасности необходимо увеличить эту величину. Внутреннее состояние RC4 представляется в виде массива слов размером 2n и двух счетчиков, каждый размером в одно слово. Массив известен как S-бокс, и далее будет обозначаться как S. Он всегда содержит перестановку 2n возможных значений слова. Два счетчика обозначены через i и j.

Этот алгоритм использует ключ, сохраненный в Key, и имеющий длину l байт. Инициализация начинается с заполнения массива S, далее этот массив перемешивается путем перестановок определяемых ключом. Так как только одно действие выполняется над S, то должно выполняться утверждение, что S всегда содержит все значения кодового слова. Реализация шифра RC4 представлена на рис.29 [34;1;35;36;37].

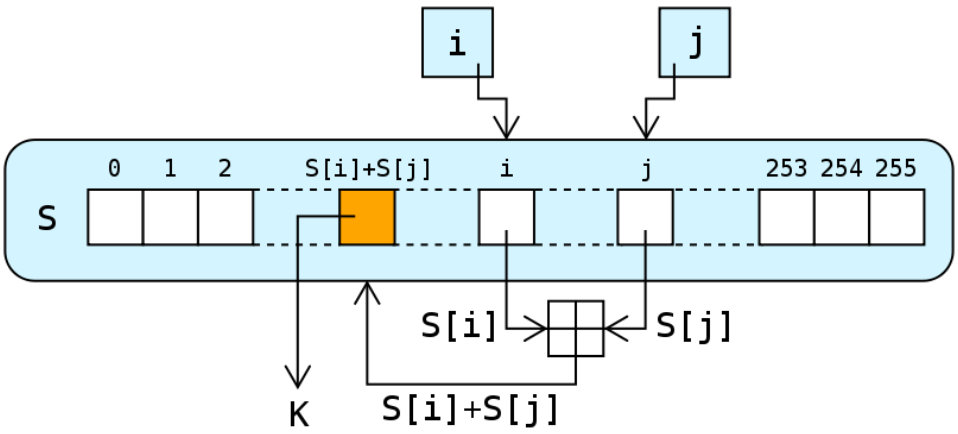


Рис.29 – Реализация шифра RC4

ШИФР SEAL. Software-optimized Encryption Algorithm (программно-оптимизированный алгоритм шифрования) – симметричный поточный алгоритм шифрования данных оптимизированный для программной реализации (рис.30).

Разработан в IBM Филом Рогэвеем и Доном Копперсмитом в 1993 году. Алгоритм оптимизирован и рекомендован для 32-битных процессоров. Для работы ему требуется кэш-память на несколько килобайт и восемь 32-битовых регистров. Скорость шифрования – примерно 4 машинных такта на байт текста. Для кодирования и декодирования используется 160-битный ключ. Чтобы избежать нежелательной потери скорости по причине медленных операций обработки ключа, SEAL предварительно выполняет с ним несколько преобразований, получая в результате три таблицы определенного размера. Непосредственно для шифрования и дешифрирования текста вместо самого ключа используются эти таблицы. Алгоритм считается очень надёжным, очень быстрым.

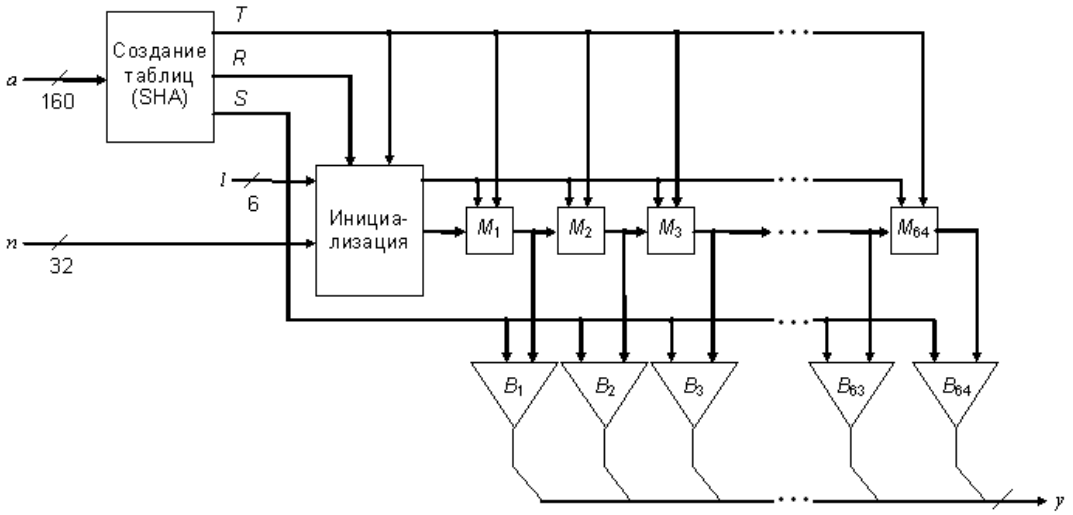


Рис.30 Реализация алгоритма SEAL

Чтобы избежать потери скорости шифрования на медленных операциях алгоритм использует три таблицы: R, S и T. Эти таблицы вычисляются с помощью процедуры из алгоритма SHA-1 и зависят только от ключа. Заполнение данных таблиц можно описать с помощью функции G, которая из 160-битной строки a и 32-битного числа i возвращает 160-битное значение $G_a(i)$. Процесс шифрования состоит из большого числа итераций, каждая из которых завершается генерацией псевдослучайной функции. Количество пройденных итераций показывает счетчик l. Все они подразделяются на несколько этапов с похожими операциями. На каждом этапе старшие 9 битов одного из регистров (A, B, C или D) используются в качестве указателя, по которому из таблицы T выбирается значение. Это значение складывается арифметически или поразрядно по модулю 2 (XOR) со следующим регистром (снова один из A, B, C или D). Затем первый выбранный регистр преобразуется циклическим сдвигом вправо на 9 позиций. Далее либо значение второго регистра модифицируется сложением или XOR с содержимым первого (уже сдвинутым) и выполняется переход к следующему этапу, либо этот переход выполняется сразу. После 8 таких этапов значения A, B, C и D складываются

(арифметически или XOR) с определенными словами из таблицы S и добавляются в ключевую последовательность y. Завершающий этап итерации заключается в прибавлении к регистрам дополнительных 32-битных значений (n1, n2 или n3, n4). Причем выбор конкретного значения зависит от четности номера данной итерации.

При разработке этого алгоритма главное внимание отводилось следующим свойствам и идеям:

- использование большой (примерно 2 Кбайта) таблицы T, получаемой из большого 160-битного ключа;
- чередование арифметических операций (сложение и побитовый XOR);
- использование внутреннего состояния системы, которое явно не проявляется в потоке данных (значения n1, n2, n3 и n4, которые изменяют регистры в конце каждой итерации);
- использование отличных друг от друга операций в зависимости от этапа итерации и ее номера.

Для шифрования и расшифрования каждого байта текста шифр SEAL требует около четырех машинных тактов. Он работает со скоростью примерно 58 Мбит/с на 32-битном процессоре с тактовой частотой 50 МГц и является одним из самых быстрых шифров.

ШИФР VMPC. Это потоковый шифр, применяющийся в некоторых системах защиты информации в компьютерных сетях [34;1;35;36;37] (рис.31). Шифр разработан криптографом Бартошем Зольтаком в качестве усиленного варианта популярного шифра RC4. Алгоритм VMPC строится как и любой потоковый шифр на основе параметризованного ключом генератора псевдослучайных битов. Основные преимущества шифра, как и RC4 – высокая скорость работы, переменный размер ключа и вектора инициализации (от 128 до 512 бит включительно), простота реализации (буквально несколько десятков строк кода).

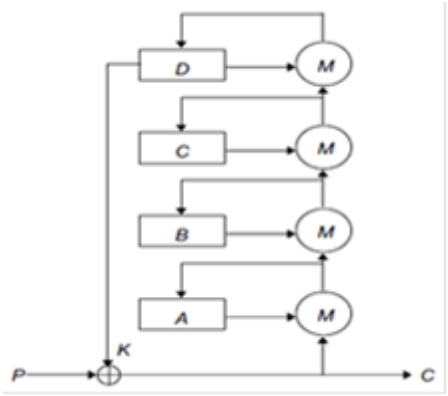


Рис.31 Реализация VMPC

Основа шифра – генератор псевдослучайных чисел, базой которого является односторонняя необратимая функция VMPC. Утверждается, что потоковый шифр, благодаря значительной модификации исходного RC4 с учетом его уязвимостей, более устойчив к существующим атакам на потоковые шифры и атакам на шифр RC4. В то

же время, безопасность большинства потоковых шифров практически сводиться к нулю при использовании одного и того же ключа для зашифрования различных открытых текстов. В таком случае потоковый шифр уже не является генератором одноразового блокнота (потока случайных бит для зашифрования открытого текста). Данная проблема шифром VMPC в некотором роде решается использованием уникального вектора инициализации для каждого зашифрованного потока.

Сложность атаки на шифр составляет 2900 операций. Однако, существует метод, защищающий алгоритм от возможных уязвимостей. Данный подход заключается в повторении зависимой от ключа перестановки два раза: до и после перестановки, зависимой от вектора инициализации. Данное ключевое расписание именуется KSA3.

ШИФР TRIVIUM. Симметричный алгоритм синхронного потокового шифрования, ориентированный, в первую очередь, на аппаратную реализацию с гибким равновесием между скоростью работы и количеством элементов, имеющий также возможность достаточно эффективной программной реализации [34;1;35;36;37].

Шифр был представлен в декабре 2008 года как часть портфолио европейского проекта eSTREAM, по профилю 2 (аппаратно ориентированные шифры). Авторами шифра являются Кристоф Де Канниэр и Барт Пренил. Данный потоковый шифр генерирует вплоть до 264 выходного потока из 80 бит ключа и 80 бит IV. Это самый простой шифр проекта eSTREAM, который показывает отличные результаты по криптоустойчивости.

Изначальное состояние Trivium представляет собой 3 сдвиговых регистра суммарной длины в 288 бит. Каждый такт происходит изменение битов в регистрах сдвига путем нелинейной комбинации прямой и обратной связи. Для инициализации шифра ключ K и инициализирующий вектор IV записываются в 2 из 3х регистров и происходит исполнение алгоритма в течение 4х288 = 1152 раз, что гарантирует зависимость каждого бита начального состояния от каждого бита ключа и каждого бита инициализирующего вектора. После прохождения стадии инициализации каждый такт генерируется новый член ключевого потока Z, который проходит процедуру XOR со следующим членом текста. Процедура расшифровки происходит в обратном порядке – каждый член шифротекста проходит процедуру XOR с каждым членом ключевого потока Z.

Стандартная аппаратная реализация алгоритма требует наличия 3488 логических элементов и производит 1 бит ключевого потока за 1 такт. Но, так как каждое новое состояние бита не изменяется по крайней мере в течение 64 раундов, то еще 64 состояния могут быть сгенерированы параллельно при увеличении количества логических элементов до 5504. Также возможны различные вариации производительности в зависимости от количества использованных элементов. Программная интерпретация данного алгоритма также достаточно эффективна. Реализация Trivium на языке C на процессоре AthlonXP 1600+ позволяет получить скорость шифрования более 2,4Мбит/с.

В отличие от ранних потоковых шифров, как например RC4, алгоритм Trivium, кроме закрытого ключа (K) также имеет инициализирующий вектор (IV), который является открытым ключом. Применение IV позволяет проводить множество независимых сеансов шифровки/расшифровки используя всего лишь 1 ключ и несколько инициализирующих векторов (по одному для каждого сеанса).

В данный момент не известно никаких методов атаки на данный алгоритм, которые были бы эффективнее последовательного перебора. Сложность проведения данной атаки зависит от длины сообщения и составляет порядка 2120.

Существуют исследования методов атак (например, кубическая атака), которые близки по эффективности к перебору. Кроме того, существует метод атаки, позволяющий восстановить K из IV и ключевого потока. Сложность данной атаки равна 2135 и незначительно уменьшается при увеличении количества инициализирующих векторов, использовавшихся с одним ключом [34;1;35;36;37]. Возможны также атаки с исследованием псевдослучайной последовательности ключевого потока с целью нахождения закономерностей и предсказания последующих бит потока, но данные атаки требуют решения сложных нелинейных уравнений. Наименьшая полученная сложность такой атаки составляет 2164.

Механизмы обеспечения ИБ в сетях 3G. Предоставление пользователям безопасного доступа к услугам 3G. Аутентификация пользователей и сети, обеспечение конфиденциальности при обмене ключами, защита информации о номере IMSI (International Mobile Subscriber Identity). Конфиденциальный обмен данными сигнализации между узлами оператора и защита от вторжений (например, подсистема противодействия мошенничеству).

Безопасный доступ к мобильным терминалам (например, аутентификация пользователь/USIM на основе PIN кода). Защищенный обмен информацией между приложениями пользователя и оператора (например, обмен сообщениями между USIM и сетью). Индикация состояния системы защиты на пользовательском уровне, позволяющая выяснить, функционирует ли средство защиты и в каком режиме.

Введение в беспроводные сети. В настоящее время существует большое количество разнообразных беспроводных технологий, что требует введения классификации. Один из способов классификации беспроводных сетей основан на радиусе действия сети, при этом выделяются четыре основных типа [34;1;35;36;37]:

•WWAN (Wireless Wide Area Network) - используются в сотовой связи (GSM, CDMA, TDMA, iDEN, PDC и др.) и характеризуются большим радиусом действия (до 40 км);

•WMAN (Wireless Metropolitan Area Network) - в основном применяются операторами связи для создания инфраструктуры доступа конечных пользователей, так называемой «последней мили», характеризуются средним радиусом действия (несколько километров);

•WLAN (Wireless Local Area Network) - используются для обслуживания небольших территорий, имеют средний радиус охвата (около 100 м);

•WPAN (Wireless Personal Area Network) - используются для передачи информации от сотовых телефонов, переносных компьютеров и т. п. бытовых приборов, имеют маленький радиус действия (около 10 м). Например, сюда можно отнести технологию Bluetooth.

Беспроводные технологии могут использоваться для решения различных задач, но в качестве основных можно выделить следующие способы их использования: - организация уровня доступа к корпоративной сети (access layer) и последней мили провайдеров сетевых услуг; - удлинение сетевого сегмента; - организация гостевого доступа и взаимодействия мобильных клиентов; - организация связи точка-точка или

точка-многоточек между зданиями; - быстрое развертывание временных локальных сетей; - обмен данными между мобильными устройствами.

Особенности радиосетей. В отличие от проводных сетей, где направление распространения сигнала определяется траекторией прокладки кабеля, а протяженность сети - длиной, беспроводные сигналы гораздо менее предсказуемы.

На качестве связи могут сказываться разнообразные факторы, от хорошо знакомой всем администраторам фазы луны, до гораздо менее понятной многолучевой интерференции.

В идеальных условиях радиосигнал распространяется от источника сигнала по прямой (что требует учета кривизны поверхности планеты при организации связи на расстояние от 12 км). Однако, на путь распространения сигнала могут влиять ряд явлений, такие как: отражение (reflection); рассеяние (scattering); преломление (refraction); дифракция (diffraction); поглощение; мнологолучевая интерференция (multipath). Значение 3 дБ указывает на увеличение мощности сигнала в два раза, а значение 10 дБ - на десятикратное увеличение мощности. То же справедливо для отрицательных величин, т.е. -3 дБ означает, что мощность уменьшилась в два раза, а -10 дБ указывает на уменьшение мощности в 10 раз [34;1;35;36;37].

Единица измерения дБи (изотропный децибел, dBi) используется для коэффициента усиления антенн. Физический смысл все тот же - десятичный логарифм отношения мощностей. Единица измерения дБм (dBm) является абсолютной величиной и отображает изменение мощности сигнала относительно фиксированного значения в один милливатт. Соответственно 1 мВт = 0 дБм. Значение 26 дБм равно мощности сигнала в 400 мВт (10 + 10 + 3 + 3). Важно помнить, что для децибелов используется правило сложения, т.е. если соединить беспроводную карточку мощности 100 мВт (20 дБм) с антенной мощностью 12 дБ (dBi), с учетом падения мощности на соединении -2 дБ, выходная мощность всей системы будет равна 1 Вт, или 30 дБм (20 + 12 - 2 = 10 + 10 + 10). Большинство используемых в настоящее время стандартов беспроводных сетей разработано Институтом инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE). Согласно приведенной выше классификации беспроводных сетей их можно разделить на персональные (WPAN), локальные (WLAN), городские (WMAN) и глобальные (WWAN) сети. Стандарты IEEE относятся только к трем последним типам беспроводных сетей.

Персональные беспроводные сети. Персональные беспроводные сети (таблица 21) находятся в ведении рабочей группы стандарта 802.15. В рамках стандарта определено четыре группы, решающие различные задачи.

Таблица 21

Стандарты 802.15.x

Стандарт	Описание
IEEE 802.15.1	Персональные беспроводные сети на основе технологии Bluetooth
IEEE 802.15.2	Совместное использование сетей WPAN с другими беспроводными технологиями
IEEE 802.15.3	Высокопроизводительные персональные беспроводные сети (High Rate WPAN)
IEEE 802.15.4	Энергосберегающие персональные беспроводные сети (Low Rate WPAN)

Стандарт IEEE 802.15.1-2002 основан на спецификации Bluetooth 1.1. В стандарте описываются канальный и физический уровни. В 2005г. была опубликована обновленная версия IEEE 802.15.1-2005. Благодаря технологиям, описанным в документе 802.15.2-2003, мы имеем возможность одновременно работать с Bluetooth и беспроводными сетями стандарта 802.11.

Протокол Bluetooth. Существует три класса устройств, поддерживающих протоколBluetooth, которые различаются мощностью передатчика [35;36] (таблица 22).

Таблица 22

Характеристики различных классов устройств

Класс	**Максимальная мощность, мВт**	**Радиус действия, м**
1	100 (20 dBm)	100
2	2,5 (4 dBm)	10
3	1 (0 dBm)	1

В протоколе используется диапазон ISM 2,4 ГГц, что позволяет работать при отсутствии прямой видимости. Поскольку данный диапазон достаточно сильно загружен, в том числе и другими беспроводными сетями, остро встает вопрос совместимости. Для снижения вероятности возникновения интерференции с другими беспроводными сетями Bluetooth используют методы частотных скачков и адаптивных частотных скачков (Adaptive Frequency Hoping Spread Spectrum, AFHSS). При этом канал (т.е. последовательность частот, между которыми переключаются приемник и передатчик), состоящий из 79 частотных подканалов в 1 МГц, постоянно изменяется на основе псевдослучайной последовательности. Поскольку количество скачков достаточно велико (до 1600/с), то мощность на каждой из частот небольшая, что снижает уровень помех для других систем. Использование метода частотных скачков требует синхронизации всех работающих устройств, что предусмотрено в спецификации стандарта Bluetooth [34;1;35;36;37].

Протокол Bluetooth поддерживает как синхронный (Synchronous Connection-Oriented, SCO), так и асинхронный режим (Asynchronous Connectionless, ACL) передачи данных. Синхронный режим используется в основном для передачи голосовой информации. Устройства, поддерживающие протокол Bluetooth 2.0, обратно совместимы с предыдущими версиям. Основным улучшением является увеличение пропускной способности до 2,1 Мбит/с (Enhanced Data Rate, ERD).

Локальные беспроводные сети. Семейство стандартов 802.11 включает в себя четыре ратифицированных стандарта, используемых для организации передачи данных, и ряд документов, описывающих дополнительные функции [1;35;36]. На время написания книги на стадии согласования находился пятый стандарт 802.11 n, направленный на увеличение пропускной способности радиосети. Семейство стандартов 802.11 часто обозначают как 802.11 x (не путать с 802.1 X) для того, чтобы не смешивать с базовым, теперь не используемым стандартом передачи 802.11.

Текущее распределение рабочих групп стандарта 802.11 приведено в таблице 23. Документы 802.11F и 802.11T не являются стандартами как таковыми, а описывают рекомендации по реализации тех или иных функций [1;35;36].

Таблица 23

Стандарт 802.11

Стандарт	**Описание**
IEEE 802.11c	Работа сетевых мостов, включен в IEEE 802.1 D (2001 г.)
IEEE 802.11d	Интернациональные расширения роуминга (2001 г.)
IEEE 802.11e	Поддержка функции обеспечения качества обслужи вания (QoS), 2005г.
IEEE 802.11F	Протокол взаимодействия между точками доступа Inter-Access Point Protocol, опубликован в 2003 г., отозван в 2006 г.
IEEE 802.11 g	Расширение стандарта 802.11Ь, поддержка скорости передачи до 54 Мбит/с в диапазоне ISM 2,4 ГГц (2003 г.)
IEEE 802.11h	Изменения используемого частотного диапазона 5 ГГц стандарта 802.11а для совместимости с европейскими требованиями (2004 г.).
IEEE 802.11 i	Расширения функций безопасности (2004 г.).
IEEE 802.11j	Изменения, связанные с требованиями Японского рынка (2004 г.).
IEEE 802.11k	Улучшения процедур радиоизмерений
IEEE 802.111 IEEE 802.11x IEEE 802.11o IEEE 802.11q	Зарезервированы и не будут использоваться в дальнейшем
IEEE 802.11m	Поддержка стандарта 802.11. Информация, не вошедшая в другие разделы
IEEE 802.11n	Высокоскоростные беспроводные сети
IEEE 802.11p	Мобильный доступ передвижных устройств (Wireless Access for the Vehicular Environment, WAVE)
IEEE 802.11r	Быстрый роуминг
IEEE 802.11s	Полносвязанные сети (ESS Mesh)
IEEE 802.11T	Управление пропускной способностью беспроводной сети (Wireless Performance Prediction, WPP). Методики тестирования и измерения
IEEE 802.11u	Взаимодействие с сетями других стандартов (сотовые сети)
IEEE 802.11V	Управление беспроводной сетью
IEEE 802.11w	Защита управляющих фреймов

Протоколы передачи данных. Первый стандарт 802.11 (без буквенного индекса, см. таблицу 23) описывает протокол организации беспроводной локальной сети в диапазоне 2,4 ГГц со скоростями 1 и 2 Мбит/с. В связи с невысокой пропускной способностью он не получил широкой поддержки со стороны производителей.

Стандарты 802.11 b/g разбивают весь частотный диапазон ISM на четырнадцать каналов, разделенных промежутком в 5 МГц (2412, 2417,..., 2477). Однако поскольку каждый канал занимает 22 МГц, не оказывают взаимного влияния те из них, номера которых различается на пять. Например, второй и седьмой (2442 - 2417= 25). Соответственно недалеко друг от друга могут находиться максимум три точки доступа, работающие на каналах 1, 6 и 11. К сожалению, большая часть оборудования

произведена в соответствии со стандартами США и поддерживает только каналы 1-11. Для исправления этой ситуации необходимо устанавливать на рабочие станции драйверы и адаптеры, произведенные не для США [1;35;36].

Когда говорят о «неперекрывающихся» каналах, немного отступают от истины. Спектральная мощность сигнала распределена по гораздо более широкому частотному диапазону, чем 22 МГц, и фактически каналы 1 и 6 перекрываются. В рамках используемых ограничений мощности передатчика этим можно пренебречь. Однако мощный передатчик на первом канале вполне может подавить сигнал стандартного клиента на шестом канале.

Региональные и городские сети. Технологии, объединенные под торговой маркой WiMAX, направлены на реализацию широкополосного беспроводного доступа на значительных расстояниях [1;35;36]. Коммерческим продвижением технологии занимается организация WiMAX Forum.

Согласно спецификации стандарта 802.16, максимальное расстояние, на котором возможно взаимодействие по сетям WiMAX, составляет 50 км, а суммарная пропускная способность - 70 Мбит/с. В условиях реальной эксплуатации эти показатели гораздо скромнее и составляют около 8 км и 2 Мбит/с. Такие характеристики делают протокол WiMAX очень привлекательным для замены традиционных технологий по предоставлению «последней мили» при доступе к сети Internet и телефонии. Провайдеры разветвленной городской беспроводной сети могут предоставлять «выделенные» беспроводные каналы для организации виртуальных частных сетей между офисами компаний. С точки зрения заказчика преимущества очевидны: большая, чем при использовании технологии DSL, пропускная способность, отсутствие необходимости прокладки кабелей, независимость от места подключения. Как правило, при переезде офиса провайдеры WiMAX предоставляют связь на тех же условиях без дополнительных формальностей [1;35;36].

В ближайшее время намечается широкое внедрение устройств стандарта 802.1 бе. Это мобильный вариант протокола WiMAX, рассчитанный на использование в качестве конечных терминалов таких устройств, как компьютеры, КПК, мобильные телефоны и т.д. На время написания книги адаптеры 802.1 бе были доступны только в виде демонстрационных прототипов. Первое масштабное внедрение мобильного варианта WiMAX происходит сейчас в Корее. Разработанный при содействии правительства стандарт WiBRO выполняет те же функции, что и стандарт 802.1 бе, и совместим с ним.

В первоначальном варианте протокола WiMAX, описанного в стандарте 802.16с использовались частоты в диапазоне 10...66 ГГц. Этому диапазону присущи некоторые ограничения, связанные с лицензированием. Кроме того, его нельзя применять в условиях наличия препятствий между приемником и передатчиком. Стандарт 802.16а, описывающий использование диапазона 2...11 ГГц вышел в 2004 г. Поскольку логика работы WiMAX предполагает применение схемы точка-многоточка с фиксированной пропускной способностью канала для каждого из абонентов, на канальном уровне используется механизм множественного доступа к несущей с разделением по времени (Time Division Multiple Access, TDMA). Этот метод широко используется в сотовых сетях (например, GSM) и позволяет реализовать гарантированное качество обслуживания. Стандарт 802.16 предполагает шифрование трафика с использованием алгоритма DES. Мобильный вариант WiMAC (802.1 бе) расширяет возможности по

защите информации, добавляя аутентификацию станций по протоколу EAP, управление ключами с использованием протокола Privacy and Key Management Protocol Version 2 (PKMv2) и шифрование AES. При использовании стандарта 802.16 для передачи корпоративных данных рекомендуется усилить встроенные механизмы защиты с помощью технологий построения виртуальных частных сетей [1;35;36].

Стандарты Wi-Fi. Существует несколько различных стандартов беспроводных соединений. На сегодняшний день основные из них такие: 802.11a, 802.11b, 802.11g и 802.11i. Отличаются эти стандарты как максимально возможной скоростью передачи данных, так и радиусом действия. В соответствии с этими стандартами выбирается и тип оборудования. В России на данный момент в подавляющем большинстве используются только два из них – это 802.11b и 802.11g. Помимо этого разрабатывается новый стандарт 802.11n, который, возможно, в скором времени станет основным.

802.11a. Оборудование, основанное на этом стандарте, и используемые им частоты не имеют сертификации на территории России. Вы конечно можете использовать его для организации домашней сети, но купить данное оборудование будет достаточно проблематично. Максимальная скорость 54 Mbps

802.11b. Хотя этот стандарт на сегодняшний день является уже довольно устаревшим, он был первым появившимся на территории России, и повсеместно используется до сих пор. Основными недостатками этого типа являются относительно невысокая скорость передачи данных и низкая степень защищенности. При желании и соответствующей квалификации, злоумышленнику не составит особых проблем расшифровать ключ, защищающий беспроводную сеть и получить к ней доступ. При работе с клиентами мы не рекомендуем использовать данный стандарт даже в домашних сетях, за исключением тех редких случаев, когда другие стандарты не поддерживаются оборудованием. Максимальная скорость 11 Mbps; Радиус действия сети 50 м; Протокол обеспечения безопасности WEP; Низкий уровень безопасности

802.11g. Это наиболее продвинутый из распространенных форматов. Он пришел на смену 802.11b и поддерживает в пять раз более высокую скорость передачи данных и гораздо более развитую систему защиты. «Обычный» 802.11g поддерживает до 54Mbps, а при использовании технологии 802.11g+ (SuperG) – 100, 108 или даже 125 Mbps. Так же значительно возрос уровень безопасности беспроводных сетей на этом стандарте. При грамотной настройке, его можно оценить как высокий. Данный стандарт поддерживает использование протоколов шифрования WPA и WPA2, которые предоставляют гораздо более высокий уровень защиты, нежели протокол WEP, использующийся в стандарте 802.11b. Максимальная скорость 54 Mbps, до 125 Mbps; Радиус действия сети 50 м; Протокол обеспечения безопасности WEP, WPA, WPA2; Высокий уровень безопасности.

802.11i. Этот стандарт появился недавно, и его распространение только начинается. В нем поддерживаются наиболее совершенные политики шифрования и передачи данных. Данный стандарт призван свести на нет все попытки взлома беспроводных сетей злоумышленниками. Максимальная скорость 125 Mbps; Радиус действия сети 50 м; Протокол обеспечения безопасности WEP, WPA, WPA2; Высокий уровень безопасности.

Несмотря на самые современные технологии, всегда следует помнить о том, что качественная передача данных и надежный уровень безопасности обеспечиваются

только правильной настройкой оборудования и программного обеспечения, выполненными опытными профессионалами. Специалисты компьютерного сервиса inetproblem.ru всегда готовы не только помочь с настройкой Вашего программного обеспечения, но и оказать высококвалифицированный срочный ремонт компьютеров.

Стандарт 802.11n. повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с (стандарт IEEE 802.11ac до 1.3 Гбит/с), применяя передачу данных сразу по четырем антеннам. По одной антенне — до 150 Мбит/с. Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц. Кроме того, устройства 802.11n могут работать в трёх режимах: - наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a; - смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n; - «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Ключевой компонент стандарта 802.11n под названием MIMO (Multiple Input, Multiple Output — много входов, много выходов) предусматривает применение пространственного мультиплексирования с целью одновременной передачи нескольких информационных потоков по одному каналу, а также многолучевое отражение, которое обеспечивает доставку каждого бита информации соответствующему получателю с небольшой вероятностью влияния помех и потерь данных [1;35;36]. Именно возможность одновременной передачи и приема данных определяет высокую пропускную способность устройств 802.11n. Радиус действия сети 50 м; Протокол обеспечения безопасности WEP, WPA, WPA2; Высокий уровень безопасности. В России этот стандарт официально сертифицирован. Оборудование стандарта 802.11n разрешено к применению на территории России в диапазонах 2400—2483.5, 5150—5350 и 5650—5725 МГц приказом Министерства связи и массовых коммуникаций России от 14 сентября 2010 г. № 124 «Об утверждении Правил применения оборудования радиодоступа. Часть I. Правила применения оборудования радиодоступа для беспроводной передачи данных в диапазоне от 30 МГц до 66 ГГц».

Безопасность wi-fi сетей. Безопасности беспроводных сетей стоит уделять особое внимание. Wi-Fi – это беспроводная сеть и притом с большим радиусом действия. Поэтому злоумышленник может перехватывать информацию или же атаковать вашу систему, находясь на безопасном расстоянии. В настоящее время существуют уже множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности [1;35;36].

Протокол шифрования WEP: Протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное шифрование [6;11;13]. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно более высокая стойкость сети к взлому. Часть WEP-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бита) – динамической (вектор инициализации), она меняется в процессе работы сети. Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и

взломщику потребуется лишь обработать эти повторы и вычислить по ним статическую часть ключа. Для повышения уровня безопасности можно дополнительно к WEP-шифрованию использовать стандарт 802.1x или VPN.

Протокол шифрования WPA: Более стойкий протокол шифрования, чем WEP , хотя используется тот же алгоритм RC4. Более высокий уровень безопасности достигается за счет использования протоколов **TKIP и MIC**.

TKIP (Temporal Key Integrity Protocol) – протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.

MIC (Message Integrity Check) – протокол проверки целостности пакетов. Защищает от перехвата пакетов и их перенаправления.

Также возможно использование 802.1x и VPN, как и в случае с протоколом WEP. Существует два вида WPA:

WPA-PSK (Pre-Shared Key) – для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети.

WPA-802.1x - вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

Протокол WPA2 - усовершенствование протокола WPA. В отличие от WPA, используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x [6;11;13].

Стандарт безопасности 802.1X, в который входят несколько протоколов:

EAP (Extensible Authentication Protocol). Протокол расширенной аутентификации. Используется совместно с RADIUS – сервером в крупных сетях.

TLS (Transport Layer Security). Протокол, который обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений.

RADIUS (Remote Authentication Dial-In User Server). Сервер аутентификации пользователей по логину и паролю.

VPN (Virtual Private Network) – Виртуальная частная сеть. Этот протокол изначально был создан для безопасного подключения клиентов к сети через общедоступные Интернет-каналы. Принцип работы VPN – создание так называемы безопасных «туннелей» от пользователя до узла доступа или сервера. Хотя VPN изначально был создан не для Wi-Fi, его можно использовать в любом типе сетей. Для шифрования трафика в VPN чаще всего используется протокол IPSec. Случаев взлома VPN на данный момент неизвестно. Рекомендуется использовать эту технологию для корпоративных сетей [1;35;36].

Дополнительные меры защиты:

- Фильтрация по MAC адресу: MAC адрес – это уникальный идентификатор устройства (сетевого адаптера), «зашитый» в него производителем. На некотором оборудовании возможно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – MAC адрес можно подменить.

- **Скрытие SSID: SSID** – это идентификатор вашей беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом при сканировании вашей сети видно не будет. Но опять же, это не слишком серьезная преграда если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в Windows.

- Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть: Активировав эту функцию можно запретить доступ к настройкам точки доступа через Wi-Fi сеть, однако это не защитит вас от перехвата трафика или от проникновения в вашу сеть.

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID (англ.)) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

По способу объединения точек доступа в единую систему можно выделить: - автономные точки доступа (называются также самостоятельные, децентрализованные, умные). Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные); - бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети: -со статическими настройками радиоканалов; - с динамическими (адаптивными) настройками радиоканалов; - со «слоистой» или многослойной структурой радиоканалов.

Недостатки Wi-Fi. В диапазоне 2.4 GHz работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др, и даже микроволновые печи, что ухудшает электромагнитную совместимость. Реальная скорость передачи данных в Wi-Fi сети всегда ниже максимальной скорости, заявляемой производителями Wi-Fi оборудования [1;35;36]. Частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. В России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации. Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенный протокол шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало доступной более безопасную схему, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Основные положения политики безопасности беспроводных сетей представлены в таблице 24.

Таблица 24

Основные положения политики безопасности беспроводных сетей

Положения политики	**Требования к безопасности**
Обучение пользователей и администраторов ISOjIEC 27001 A.8.2.2	Пользователи должны знать и понимать изложенные в политике ограничения, а администраторы должны иметь необходимую квалификацию для предотвращения и обнаружения нарушений политики
Контроль подключений к сети ISO|IEC 27001 A. 11.4.3	Уровень риска, связанного с подключением несанкционированной точки доступа или клиента беспроводной сети, можно снизить путем отключения неиспользуемых портов коммутаторов, фильтрации по MAC-адресам (port-security), аутентификации 802.1X, систем обнаружения атак и сканеров безопасности, контролирующих появление новых сетевых объектов
Физическая безопасность ISO|IEC 27001 A.9.1	Контроль приносимых на территорию устройств позволяет ограничить вероятность подключения к сети беспроводных устройств. Ограничение доступа пользователей и посетителей к сетевым портам и слотам расширения компьютера снижает вероятность подключения беспроводного устройства
Минимизация привилегий пользователя ISO|IEC 27001 A.11.2.2	Если пользователь работает на компьютере с минимально необходимыми правами, то снижается вероятность самовольного изменения настроек беспроводных интерфейсов
Контроль политики безопасности ISOjIEC 27001 6, A.6.1.8	Средства анализа защищенности, такие как сканеры уязвимостей, позволяют обнаруживать появление в сети новых устройств и определять их тип (функции определения версий ОС и сетевых приложений), а также отслеживать отклонения настроек клиентов от заданного профиля. Техническое задание на проведение работ по аудиту внешними консультантами должно учитывать требования политики в отношении беспроводных сетей
Инвентаризация ресурсов ISOjlEC 27001 A.7.1.1	Наличие актуального обновляемого списка сетевых ресурсов облегчает обнаружение новых сетевых объектов
Обнаружение атак ISO|lEC 27001 A.10.10.2	Применение систем обнаружения как традиционных, так и беспроводных атак дает возможность своевременно определять попытки несанкционированного доступа
Расследование инцидентов ISOjlEC 27001 A.13.2	Инциденты, связанные с беспроводными сетями, мало отличаются от других подобных ситуаций, однако процедуры их расследования должны быть определены

Окончание таблицы 24

Положения политики	Требования к безопасности
Нормативно-правовое обеспечение ISO|IEC 27001 A.15.1.1	Использование беспроводных сетей может попадать под действие как российских, так и международных нормативных актов. Так, в России использование частотного диапазона 2,4 ГГц регулируется решением ГКРЧ от 6.11.2004 (04-03-04-003). Кроме того, поскольку в беспроводных сетях интенсивно используется шифрование, а применение крипто-графических средств защиты в ряде случаев попадает под довольно жесткие законодательные ограничения, необходимо проработать и этот вопрос
Внутренний и внешний аудит ISOjlEC 27001 6, A.6.1.8	При проведении работ по оценке защищенности должны учитываться требования политики в отношении беспроводных сетей.
Разделение сетей ISOjlEC 27001 A.11.4.5	В связи со спецификой беспроводных сетей желательно выделять точки беспроводного доступа в отдельный сетевой сегмент с помощью межсетевого экрана, особенно когда речь касается гостевого доступа
Использование криптографических средств защиты 1S0|IEC 27001 A.12.3	Должны быть определены используемые протоколы и алгоритмы шифрования трафика в беспроводной сети (WPA или 802.11 i). При использовании технологии 802.1X определяются требования к протоколам ЭЦП и длине ключа подписи сертификатов, используемых для различных целей
Аутентификация ISOjIEC 27001 A.11.4.2	Должны быть определены требования к хранению данных аутентификации, их смене, сложности, безопасности при передаче по сети, а также должны быть явно определены используемые методы EAP, методы защиты общего ключа сервера RADIUS
Контроль изменений в информационной системе ISO)IEC 27001 A.12.5.1	Должны учитываться используемые в ИС беспроводные технологии
Допустимость использования программного и аппаратного обеспечения. ISOjIEC 27001 A.12.4.1	В этом разделе рассматриваются требования к точкам доступа, беспроводным коммутаторам и клиентам беспроводной сети
Обнаружение атак ISO|IEC 27001 A.10.10.2	Должны быть определены требования к системам обнаружения беспроводных атак, закреплена ответственность за анализ событий
Протоколирование и анализ событий безопасности ISO|IEC 27001 A.10.10.1	Данный раздел может быть расширен путем добавления в список контролируемых событий, специфичных для беспроводных сетей. Может включать в себя предыдущий раздел
Удаленный доступ к сети - ISOjIEC 27001 A.11.7.2	В большинстве случаев пользователей беспроводной сети логично относить к пользователям систем удаленного доступа. Это обусловлено аналогичными угрозами и как следствие - контрмерами, характерными для данных компонентов ИС

Кроме того, в том или ином виде должны быть сформированы следующие документы: инструкция для пользователей с учетом использования беспроводной сети; базовые настройки точек доступа, беспроводных коммутаторов, рабочих станций; процедуры контроля защищенности беспроводных сетей; профили систем обнаружения атак; процедуры по реагированию на инциденты в беспроводной сети [1;35;36].

Правильно построенная и соблюдаемая политика безопасности является надежным фундаментом защищенной беспроводной сети. Вследствие этого стоит уделять ей достаточное внимание, как на этапе внедрения сети, так и в ходе ее эксплуатации, отражая в нормативных документах изменения, происходящие в сети.

Базовые механизмы защиты. При разработке в стандарт 802.11 были заложены некоторые функции, которые могут быть использованы в качестве защитных механизмов. Несмотря на то, что их эффективность гораздо ниже таких мощных средств как 802.1 X и 802.11 i, некоторые из них должны учитываться при проектировании беспроводной сети. К таким механизмам относятся: ограничение зоны распространения радиосигнала; списки контроля доступа на основе списков MAC-адресов; отключение широковещательной рассылки идентификатора сети; изменение стандартных настроек; защита точек доступа [1;35;36].

Контроль границы сети. Ограничение зоны распространения радиосигнала позволяет решить две задачи: снизить вероятность обнаружения радиосети и уменьшить расстояние, с которого злоумышленник может осуществлять активные или пассивные атаки. Естественно, что для злоумышленника, вооруженного направленной параболической антенной с усилением в 24 дБи, нет ничего невозможного, но большинство любителей бесплатного доступа к Internet просто не заметят существования такой сети. Да и мало найдется любителей, носящих с собой грозное метровое орудие. Ограничить зону распространения радиосигнала границами физического периметра практически невозможно. Однако при проектировании и развертывании радиосети стоит учитывать вопросы минимизации уровня сигнала. К счастью, современные подходы к организации высокоскоростных радиосетей по сотовому принципу с чередованием каналов согласно мантре 1-6-11 также требуют ограничения мощности передатчиков для снижения интерференции на точках доступа, работающих на одинаковых каналах.

Для ограничения радиуса охвата радиосети могут использоваться такие методы и средства как аттенюаторы, снижение мощности передатчика встроенными средствами точки доступа, использование направленных антенн и просто правильная ориентация антенн в пространстве. Эффективным способом является выбор места размещения точек доступа в отдалении от границ здания. Кроме того, современные системы обнаружения беспроводных атак могут использовать функцию определения координат устройства для предотвращения соединения из-за пределов физического периметра.

Для сетей с высокими требованиями к безопасности могут применяться дополнительные методы, такие как покраска стен помещений с помощью специальной краски, обладающей высоким коэффициентом поглощения в частотном диапазоне, используемом радиосетями. Достаточно радикальным методом, применяемым в серверных комнатах, или в других критичных помещениях является установка помехи в частотном диапазоне радиосетей. Для этого используются специализированные генераторы шума [1;35;36].

Списки контроля доступа. Большинство точек доступа и беспроводных коммутаторов позволяет указывать черные и белые списки MAC-адресов станций, которым запрещено (или разрешено) подключаться к сети. В результате при попытке установления ассоциации проверяется, разрешено ли станции с таким MAC-адресом подключатся к сети, и если нет, то отсылается фрейм Disassociate. Поскольку вопреки распространенному заблуждению MAC-адрес не является уникальной и неотъемлемой характеристикой сетевого адаптера, ограничение доступа по MAC-адресам достаточно просто обойти. Для этого злоумышленник может отредактировать MAC адрес в свойствах сетевого адаптера или изменить его путем редактирования ключа реестра

В случае использования Linux изменение MAC-адреса является штатной функцией утилиты ifconfig. Однако, несмотря на это, в большинстве случаев есть смысл задействовать данный механизм. Во-первых, для того, чтобы осуществить подключение, злоумышленник должен знать MAC-адрес разрешенного клиента. Получить его, прослушав сеть в режиме мониторинга, не представляет особого труда. Однако если в сети отсутствуют клиенты (например, в нерабочее время), злоумышленнику остается только осуществлять подбор по адресному пространству в 2^{48}. Согласитесь, пытаться осуществить несколько миллионов подключений довольно неблагодарное занятие (хотя эта техника и используется для взлома устройств Bluetooth). На практике, за счет того, что идентификаторы производителей беспроводных карт (OUI) хорошо известны, пространство для перебора гораздо меньше, и составляет менее 2^{24}.

Во-вторых, данный защитный механизм весьма эффективен в качестве детективного средства защиты. Поскольку большинство точек доступа ведет журналы попыток несанкционированного доступа и поддерживает протокол Syslog, можно воспользоваться штатными возможностями системы обнаружения атак или корреляции

Рассылка SSID. В служебных фреймах Beacon и Probe Response точка доступа отправляет идентификатор сети и другие служебные данные. Именно эту информацию выводят стандартные утилиты подключения к беспроводной сети и многочисленные «стамблеры». Стандартом предусмотрена и в большинстве точек доступа реализована возможность отключать широковещательную рассылку SSID. Этот режим обычно называется disable ssid broadcast или no guest mode. В результате в поле SSID во фреймах Beacon и Probe Response будет указываться пустая строка. Такие сети не будут отображаться в утилитах типа Netstumbler и не будут видны в списке доступных сетей стандартного беспроводного клиента. В результате может возникнуть ощущение, что таким образом удастся скрыть сеть от злоумышленника, который не знает ее SSID [1;35;36].

Но задача поиска сети по ее идентификатору остается нерешенной, и, поскольку она не реализуется точкой доступа, ее берут на себя станции беспроводной сети. Для этого клиенты рассылают в запросах Probe Request идентификаторы сетей, указанные в профиле подключения. Если точка доступа отвечает на такой фрейм, значит, ее SSID совпадает со значением, указанным в запросе, и можно приступать к процедуре подключения. В результате злоумышленник, прослушивающий сеть в режиме мониторинга, получает возможность узнавать идентификатор сети. Существует большое количество утилит, работающих по такому принципу, например, популярный анализатор беспроводных сетей Kismet.

С их помощью довольно просто узнать идентификатор «скрытой» сети, если с ней работают клиенты. Кроме того, такая логика работы станции приводит к разглашению настроек профиля беспроводных подключений клиента, поскольку он вынужден рассылать SSID с конфигурированных станций. Таким образом, прекращение широковещательной рассылки идентификатора сети не является серьезным средством защиты, разве что может снизить количество срабатываний системы обнаружения атак, связанных с попытками подключения совсем уж неумелых «хакеров». Однако, поскольку большинство беспроводных клиентов рассылает SSID сети в запросах на подключение независимо от типа точки доступа, возможно, есть смысл использовать эту возможность.

Механизмы защиты технологии Bluetooth. В зависимости от настроек устройство Bluetooth может поддерживать различный уровень защиты при доступе к своим службам.В стандарте описаны три режима безопасности:

- режим 1 (Mode 1), отсутствие защиты;
- режим 2 (Mode 2), защита на уровне приложений (L2CAP);
- режим 3 (Mode 3), аутентификация и шифрование трафика.

Как правило, режимы безопасности настраиваются для каждой из служб индивидуально. Работа в третьем режиме требует настройки сопряжения устройствами (pairing). Во время сопряжения устройства проходят взаимную аутентификацию с использованием общего ключа (PIN) и в случае, если процесс прошел успешно, сохраняют информацию о партнере в профиле подключения. Дальнейшие соединения происходят уже без ввода PIN. Работа в режиме партнерских отношений позволяет не только реализовывать взаимную аутентификацию, но и зашифровывать передаваемые между устройствами данные. Большинство устройств может быть настроено на обязательную аутентификацию при обмене [1;35;36]. Однако многие сотовые телефоны принимают контакты по протоколу OBEX без аутентификации. Такие же стандартные настройки могут существовать в устройствах других типов, например принтерах, принимающих задачи на печать без аутентификации. Популярный стек Bluetooth для Windows Broadcom/Widcomm также принимает визитные карточки без аутентификации и сохраняет их в качестве контакта в Outlook Express.

Режим Mode 3. При работе в этом режиме все взаимодействия происходят в рамках аутентифицированного и зашифрованного канала связи. Для выполнения криптографических преобразований в устройствах Bluetooth используется шифр под кодовым названием E0 (SAFER+). Этот алгоритм был специально разработан для использования в Bluetooth. Алгоритм E0 представляет собой блочный шифр с длиной ключа 128, 192 и 256 бит. В современных реализациях Bluetooth используется длина ключа 128 бит. Однако исследования показали, что эффективная сила ключа для E0-128 составляет около 84 бит.

Уязвимости устройств Bluetooth. Как видно из предыдущего изложения, протокол Bluetooth обладает достаточно надежными механизмами безопасности, включающими в себя методы противодействия несанкционированным подключениям (аутентификация) и прослушиванию трафика (шифрование). Однако, при анализе деталей реализации или стандартных настроек стеков Bluetooth различных производителей выясняется, что все далеко не так хорошо. Протокол Bluetooth может использоваться для разнообразных атак, направленных на нарушение

конфиденциальности, целостности и доступности. В следующих разделах описываются наиболее известные уязвимости реализаций стека Bluetooth различных производителей.

Bluejacking. Под термином Bluejacking подразумевается анонимное общение с помощью Bluetooth. Как правило, развлекаются Bluejacking в таких местах как общественный транспорт, торговые центры, кинотеатры. Сообщения посылаются в поле имени устройства или в визитной карточке, передаваемой посредством OBEX. В случае использования имени устройства на принимающей стороне появляется запрос на подключение с текстом, указанным инициатором общения [1;35;36].

Поскольку многие сотовые телефоны принимают визитные карточки без авторизации, независимо от настроек, они также могут использоваться для обмена сообщениями. После первоначального обмена любезностями обе стороны имеют возможность выполнить процедуру сопряжения и обмениваться фотографиями, музыкой и другими способами нарушать закон об авторских и смежных правах, В большинстве случаев Bluejacking представляет собой модную, высокотехнологичную и безобидную забаву. Однако, как всякое человеческое общение, такие разговоры могут вызывать и негативные эмоции. Это связано с сообщениями оскорбительного, экстремистского, рекламного характера. Телефонные хулиганы нашли себе новую нишу. Хотя в случае Bluetooth подобный «синезубый» агрессор довольно сильно рискует, поскольку десяти метров, отделяющих его от жертвы явно недостаточно для того, чтобы воспрепятствовать переходу от общения высокотехнологического к более тривиальным методам выяснения отношений.

Bluenibbling. Термин Bluenibbling обозначает свободный поиск устройств Bluetooth и сбор информации о них. По своей сути Bluenibblingочень похож на «боевые выезды», направленные на обнаружение и позиционирование беспроводных точек доступа, Wardriving. Технически такие работы представляют собой постоянное сканирование эфира в поиске устройств, отвечающих на широковещательные запросы подключения. Как уже говорилось ранее, большинство устройств могут быть настроены таким образом, что не будут отвечать на широковещательные запросы.

Для того, чтобы устройство ответило, запрос inquire должен быть направлен на его MAC-адрес. Для того, чтобы Выяснить адрес устройства, не поддерживающего обнаружение, можно воспользовавшись активным и пассивным подходами.

Активный поиск устройств представляет собой подбор MAC-адреса, т.е. злоумышленник последовательно посылает запросы на различные адреса. Впервые эта техника была предложена Олли Вайтхаузом (Ollie Whitehouse). Со временем она получила развитие в части оптимизации адресного пространства и распараллеливания процесса. С точки зрения оптимизации пространства перебора могут использоваться хорошо известные списки OUI, содержащие три первых октета MAC-адреса. Некоторые модели устройств имеют еще более ограниченный диапазон адресов. Например, MAC-адреса телефона Sony Ericsson P900 в большинстве случаев начинаются с префикса 00:0A:D9:E. Что касается распараллеливания процесса перебора, использование нескольких Bluetooth-устройств позволяет в несколько раз

увеличить скорость подбора. Последние версии redfang могут использовать до восьми устройств для одновременной проверки различных адресов.

Пассивные методы поиска устройств могут быть использованы двумя путями. Один из них - перевод своего устройства в режим ожидания подключений и анализ поступающих запросов, другой - использование уже упоминавшихся выше анализаторов Bluetooth. Однако, для того, чтобы устройство начало искать другие, в большинство случаев требуется инициатива со стороны пользователя. Эти действия можно спровоцировать различными методами, например, путем установки широкополосной радиопомехи в частотном диапазоне ISM. Отсутствие связи с гарнитурой/телефоном/КПК наверняка заставит пользователя проверить свои настройки и попытаться установить соединение заново.

Набор параметров, которые могут быть использованы для определения устройства, достаточно стандартен: MAC-адрес отправителя по списку OUI; имя устройства; идентификатор чипа, переданный при опросе; набор поддерживаемых устройством возможностей; информация о поддерживаемых сервисах, полученная по SDP.

Защита устройств Bluetooth. Комплекс мероприятий по защите устройств Bluetooth тривиален. Стоит отключать функцию обнаружения устройства и включать ее только при необходимости сопряжения с новым устройством. В некоторых телефонах это реализовано следующим образом: функция обнаружения активизируется только на 60 с, после чего автоматически отключается. Эта контрмера не является абсолютной защитой, но достаточно эффективна в большинстве случаев. На более интеллектуальных, чем сотовые телефоны, устройствах, как правило, имеется возможность настройки предоставляемых сервисов. Стоит отключать те из них, которые не используются на данном конкретном устройстве. Для тех сервисов, которые активно используются, необходимо требовать использования режима 3 (Mode 3) и, возможно, дополнительной авторизации [1;35;36]. Инструменты для защиты Bluetooth представлены в таблице 25.

Что касается процесса сопряжения, его желательно проводить только с доверенными устройствами в приватных местах. Хотя выполнить последнюю часть рекомендаций достаточно сложно в связи с расплывчатостью понятия «приватное место», не стоит впадать в панику. Не забывайте про стоимость анализатора трафика для Bluetooth. Десять тысяч долларов сами по себе являются эффективной контрмерой.

Периодически проверяйте список сопряженных устройств на предмет наличия незнакомых записей и безжалостно вычищайте те из них, которые не узнали с первого раза. Не забывайте про управление обновлениями безопасности. Патчи выходят не только для Windows, но и для сотовых телефонов и КПК. Хотя, конечно устанавливаются они гораздо реже. Интересным источником информации об уязвимостях в беспроводных устройствах, в том числе и в Bluetooth, является сайт Wireless Vulnerabilities & Exploits. По функциям он претендует на CVE беспроводного мира, но пока является скорее дополнительным источником информации, чем основным.

Таблица 25

Инструменты для работы с Bluetooth

Название	**Платформа**	**Описание**
BlueZ	Linux	Стек протоколов Bluetooth. Утилиты hciconfig,hcidump, hcitooi, obexftp и т.д. http://www.BlueZ.org/
btsacnner	Linux	Обнаружение устройств, подбор адресов, пассивный поиск уязвимостей (Bluesnarf) http://www.pentest.co.uk/cgibin/viewcat.cgi?cat=downloads
BTScanner XP	Windows XP	Обнаружение устройств http://www.pentest.co.uk/cgibin/viewcat.cgi?cat=downloads
BlueSweep	Windows XP	Обнаружение устройств http://www.airmagnet.com/products/bluesweep.htm
RegFang	Linux	Подбор адресов http://www.net-security.org/sottware. php?id=519
Bluesniff	Linux	Подбор адресов, пассивный сбор адресов http://bluesniff.shmoo.com/
Blueprint	Linux	Идентификация устройств http://trifinite.org/Downloads/bp_v01-2.zip
Blooover li	J2ME	Набор эксплойтов http:/Arifinite.org/trifinite_downloads.html
BlueDiving	Linux	Набор эксплойтов, инструменты для поиска уязвимостей http://bluediving.sourceforge.net/
Bluetooth Stack Smasher	Linux	Fuzzer для L2CAP http://www.secuobs.com/news/05022006- bluetoothlO.shtml
BTCrack	Windows	Подбор PIN-кодов http://secdev.zoller.lu/

Таким образом, протокол Bluetooth является достаточно защищенным сам по себе. Использование встроенных средств защиты таких как отключение функции обнаружения, шифрование трафика и аутентификация устройств, позволяет реализовать его без лишних проблем.

Межсетевое экранирование беспроводной сети. Фильтрация трафика беспроводной сети на межсетевых экранах может использоваться для решения следующих задач: - сегментация сети; - ограничение взаимодействия между сетями и контроль нарушений политики безопасности; - разделение гостевого доступа и аутентифицированного доступа; - дополнительная аутентификация клиентов; - биллинг. Выделение беспроводной сети в отдельный сегмент или WLAN само по себе ограничивает возможности злоумышленника в случае компрометации сети. Ряд широко используемых злоумышленниками атак, таких как ARP-spoofing, ICMP-Redirect, ложный сервер DHCP и т.д., могут быть реализованы только в рамках одного широковещательного сегмента. Правильно построенная политика фильтрации трафика позволяет минимизировать последствия компрометации беспроводной сети и своевременно обнаруживать попытки несанкционированного доступа.

Кроме того, разделение сетей позволяет повысить производительность беспроводной сети путем отсечения на межсетевом экране паразитного широковещательного трафика из проводного сегмента, такого как пакеты ARP, DHCP, NetBIOS и прочее [1;35;36]. Однако эти же меры могут повлечь и ряд негативных эффектов, например, падение производительности беспроводной сети за счет задержек на межсетевом экране и возникновение проблем при обработке групповых рассылок, а также проблемы с некоторыми прикладными протоколами. В связи с этим следует скрупулезно подойти к вопросам проектирования, внедрения и эксплуатации «беспроводного» брандмауэра.

Проектирование подсистемы межсетевого экранирования беспроводной сети мало чем отличается от аналогичной операции для случаев подключения к внешним сетям или формирования демилитаризованной зоны. Необходимо определить топологию подключения, тип используемого межсетевого экрана, принять решение об использовании трансляции адресов и сформировать политику фильтрации трафика.

Топология сети. Разнообразие различных схем размещения межсетевого экрана (МСЭ) для беспроводной сети можно свести к двум основным вариантам: когда беспроводная сеть выносится в демилитаризованную сеть (ДМЗ), формируемую граничными межсетевыми экранами, или когда для фильтрации используется выделенный МСЭ, подключенный к локальной сети. Первую из приведенных схем подключения удобно использовать при небольшом объеме трафика в беспроводной сети.

Атаки на пользователей WLAN. Как и в проводных сетях, где усиление защиты серверов привело к смещению внимания злоумышленников на рабочие станции пользователей, применение WPA и 802.11 i вынуждает атакующих искать обходные пути использования беспроводных сетей для взломов. Надо отметить, что точно так же как и в традиционных сетях, атаки на клиентов беспроводных сетей по эффективности могут превосходить традиционный взлом защиты точек доступа [1;35;36].

Можно выделить четыре основные угрозы безопасности, связанные с мобильными клиентами: атаки на ОС и прикладное ПО клиентов беспроводной сети; перехват трафика при использовании незащищенных беспроводных соединений; атаки «человек посередине», которые могут быть использованы для реализации других атак; использование беспроводных клиентов в качестве канала удаленного доступа к корпоративной сети. Конечно, существует ряд других проблем, связанных с мобильными клиентами, например кража устройств и т.д., однако мы остановимся на тех из них, которые специфичны именно для беспроводных сетей. При использовании для защиты беспроводной сети технологий VPN или при подключении к Internet возникает ситуация, о которой мечтают многие злоумышленники: атакуемый находится с ним в одном сегменте. Возможность подключиться к той же точке доступа, что и клиент, позволяет реализовать атаки, использующие перенаправление трафика (внедрение ложного маршрута), такие как: удаленное изменение таблицы ARP (ARP-Spoofing); внедрение ложного DHCP сервера; внедрение ложного сервера DNS или подмена DNS-ответов (DNS-spoofing); изменение таблицы маршрутизации (ICMP

Redirect); внедрение ложного шлюза по умолчанию через сообщения Neighbor Advertisement (в случае использования IPv6).

В результате злоумышленник, направив трафик через свой узел, получает возможность модифицировать данные, передаваемые между клиентом и серверами, и даже реализовать атаки на криптографические протоколы защиты данных, например атаку «человек посередине», против протоколов SSL, SSH и RDP или атаки на понижение уровня защиты протокола PPTP. Установленный на компьютере злоумышленника HTTP-посредник выполняющий также функции DNS сервера и шлюза по умолчанию для клиента, может заменять рекламные блоки на загружаемых Webстраницах на WMF-файл, эксплуатирующий уязвимость CVE-20054560 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560), и устанавливать на машину пользователя троянские программы. Для этого не понадобится никаких специализированных «хакерских» программ. Вполне достаточно обыкновенных серверов DHCP, DNS, HTTP-посредника и функций маршрутизации ОС. Хотя, конечно, можно использовать специализированные утилиты, такие как DHCP Gobbler, ettercap, Karma, airsnarf или Cain. Естественным методом защиты в таких ситуациях является использование персонального межсетевого экрана или системы предотвращения атак уровня узла [1;35;36].

Ложная точка доступа. Если пользователь работает с беспроводной сетью, использующей технологии WPA или 802.11 i, ситуация с точки зрения злоумышленника усложняется, но не становится абсолютно безнадежной [1;35;36]. Один из эффективных способов обхода защиты беспроводной сети заключается в использовании дополнительных профилей подключения, зачастую присутствующих на клиентских рабочих местах. Большинство мобильных пользователей подключается не только к беспроводной сети компании, но и настраивают свою рабочую станцию на доступ к менее защищенным сетям, например к домашней беспроводной сети. В зависимости от используемой реализации клиента беспроводных сетей и его настроек злоумышленник имеет возможность получить информацию об используемых клиентом подключениях. Клиент беспроводных сетей в ОС семейства Windows реализован в виде системной службы Wireless Zero Configuration (wzcsv) и работает по следующему алгоритму:

1. Составляется список доступных сетей путем рассылки запросов Probe Request с пустым значение SSID по всем каналам.
2. Последовательно рассылаются запросы Probe Request с указанием SSID сетей, указанных в свойствах клиента и присутствующих в списке доступных сетей. Порядок опроса сетей задается их порядком в списке preferred networks.
3. Если ни одна из сетей не ответила на запрос или соединение с сетью не было установлено, опрашиваются сети, которые отсутствуют в списке доступных сетей, что позволяет определить наличие сети, не рассылающей идентификатор во фреймах Beacon и Probe Response.

4. В случае если ассоциация с точками доступа не была установлена и соединение с одноранговыми сетями не запрещено (не включен режим Access point networks only) проводится попытка установить соединение Ad-Hoc сетями, которые указаны в свойствах клиента.

5. Если одноранговые сети не обнаружены, клиент настраивает беспроводной интерфейс в качестве первого узла такой сети и ожидает подключения других клиентов.

6. В случае если подключение к сетям Ad-Hoc запрещено, Wireless Auto Configuration проверяет значение параметра Automatically Connect To Non-Preferred Networks (по умолчанию этот режим отключен). Если данная опция отключена, то адаптер переходит в режим инфраструктуры со случайным значением SSID.

7. Если параметр Automatically Connect To Non-Preferred Networks равен единице, клиент беспроводных сетей пытается соединиться с доступными сетями, полученными при опросе радиоэфира.

В случае сбоя подключения цикл повторяется через 60 с.

Логика работы клиента беспроводной сети подсказывает и логику действий злоумышленника.

1. Если клиент соединен с точкой доступа, он отключается от нее.

2. Трафик беспроводной сети прослушивается с целью получения списка сетей, на работу с которыми настроен клиент (пункты 2, 3 и 4 работы клиента).

3. На основе полученных данных злоумышленник настраивает ложную точку доступа с SSID, полученным в пункте 2. При этом клиент отключается от других точек доступа.

4. Если предыдущий этап не был успешен, то с помощью настройки ложной точки доступа с заранее настроенным SSID злоумышленник проверяет, настроен ли клиент на соединение с любыми точками доступа (Automatically Connect To Non-Preferred Networks, пункт 7) и уязвимость пользователя к атакам с использованием социальной инженерии.

5. Если клиент не установил соединение ни с одной из предложенных сетей, злоумышленник дожидается момента, когда клиент перейдет в состояние 6, извлекает из пакета Probe Request случайное значение SSID и устанавливает точку доступа с этим значением.

Аналогичных результатов можно достичь, используя точку доступа, отвечающую на любой запрос Probe Request, без анализа указанного в пакете значения SSID [1;35;36]. Именно таким образом работает утилита Karma Tools. Что касается пятого пункта действий злоумышленника, то возможность соединения с точкой доступа со случайным значением SSID зависит от используемого беспроводного адаптера. Например, популярные карточки D-link (по крайней мере, линейки DWL-520) прекрасно ассоциируются с точкой доступа, даже если в профиле подключения не указано ни одной сети. Если хотя бы одна из сетей использует незащищенное соединение, сценарий действия злоумышленника мало отличается от описанного ранее:

- настройка IP-адреса на клиенте с помощью ложного DHCP сервера, сообщений Router Advertisement в IPv6 или определение назначенного адреса путем прослушивания трафика клиента (например, широковещательных запросов NetBIOS или UPNP);
- атаки на клиентское или серверное программное обеспечение рабочей станции, фишинг и т.д.

В ситуации, когда клиент использует для защиты соединений WEP, злоумышленник может пойти по накатанной дороге получения ключа шифрования путем анализа пакетов с различными векторами инициализации. Для этого может быть использовано пассивное прослушивание трафика (если клиент настроен на работу в режиме Ad-Hoc, он будет периодически рассылать зашифрованные широковещательные запросы NetBIOS) либо активные атаки.

Неконтролируемое использование беспроводных сетей. Возможность поддержки беспроводных соединений в стандартных сетевых устройствах создает неконтролируемый канал утечки информации, пробивая бреши в периметре корпоративной сети [1;35;36]. Можно подключить к локальной сети беспроводную точку доступа или настроить на своем ноутбуке сетевой мост между беспроводным адаптером и локальной сетью. Можно забыть отключить беспроводной адаптер после работы с домашней сетью и т.д. Все это дает внешнему злоумышленнику возможность получения доступа к корпоративным данным.

Зачастую приходится сталкиваться с ситуациями, когда ушлые пользователи, неудовлетворенные жесткой политикой фильтрации трафика на корпоративном межсетевом экране, находили доступные с рабочего места беспроводные сети и (не всегда легально) использовали их для подключения к Internet. Разве это не мечта любого злоумышленника: рабочая станция, одновременно подключенная к контролируемой им сети (а любая незащищенная беспроводная сеть потенциально контролируется злоумышленником) и к корпоративным ресурсам?

Уязвимости драйверов. Программное обеспечение драйверов и «прошивки» (firmware) беспроводных сетевых адаптеров гораздо сложнее программы «Hello World», что повышает вероятность возникновения различных ошибок [1;35;36].

Одной из уязвимостей является возможность установления соединения в «припаркованном» режиме. Как уже говорилось ранее, в этот режим адаптер устанавливается в случае, если не было обнаружено ни одной подходящей сети. В «припаркованном» режиме адаптеру присваивается случайное значение SSID, и по логике вещей он не должен соединяться ни с одной сетью. Поскольку SSID продолжает рассылаться в запросах Probe Request, злоумышленник может построить точку доступа, отвечающую на такие пакеты, и установить соединение со станцией.

Драйверы беспроводных устройств гораздо сложнее программы «Hello World» и в них вполне могут содержаться различного рода ошибки, в том числе и приводящие к проблемам с безопасностью.

Защита мобильных пользователей. Рекомендации по защите от описанных атак довольно просты: компьютеры беспроводных клиентов должны быть защищены с помощью персональных межсетевых экранов или систем предотвращения атак; клиент не должен соединяться с произвольными сетями (Automatically Connect To Non-Preferred Networks); профиль беспроводных сетей клиента не должен содержать незащищенных сетей; при работе с сетями, контролируемыми третьими лицами, должна использоваться технология VPN; пользователь, подключенный к корпоративной сети, не должен использовать беспроводной адаптер, настроенный на работу с другими сетями; на клиентские компьютеры должны быть установлены последние обновления безопасности ОС и драйверов; неконтролируемое подключение к корпоративной сети точек доступа и других беспроводных устройств должно быть запрещено.

Персональные системы обнаружения атак. Как было показано ранее, одной из наиболее распространенных атак на клиентов беспроводной сети является установка ложной точки доступа, а наиболее надежный способ защиты от таких атак правильное использование аутентификации на основе 802.1 X [1;35;36]. Однако если пользователь подключается к сети Internet через общедоступную сеть в аэропорту или через беспроводную сеть провайдера, как правило, ни о какой стойкой аутентификации не может быть речи. Для контроля текущего состояния беспроводного адаптера можно воспользоваться персональными системами обнаружения беспроводных атак. Как и персональная IDS или персональный межсетевой экран подобное программное обеспечение устанавливается на каждый компьютер пользователя и может контролировать его безопасность даже в случае работы вне офиса.

Теоретически персональная беспроводная система IDS может выполнять следующие функции: - контролировать SSID сетей, с которыми работает пользователь; - определять тип точки доступа, с которой установлено соединение; - извещать пользователя и блокировать использование опасных настроек; - извещать пользователя и блокировать атаки на канальном уровне; - вести журналы работы пользователя с беспроводными сетями; - работать с системой централизованного управления основной беспроводной IDS. Однако особенность реализации стека беспроводных сетей в ОС Windows не позволяет реализовать функции обнаружения атак в полной мере, поскольку без создания собственного драйвера практически невозможно получить доступ к содержимому управляющих фреймов 802.11 [1;35;36].

Конечно, система обнаружения атак может расшифровать трафик WEP, WPA или 802.11i в случае использования для аутентификации статических ключей, но в корпоративной сети это скорее исключение, чем правило. Если в сети используется аутентификация 802.1 X, система обнаружения атак просто не имеет доступа к ключам шифрования и не может анализировать данные и заголовки более высоких уровней, чем канальный. В таблице 26 приведен список атак [1;35;36], обнаруживаемых системами AirMagnet.

Таблица 26

Атаки, обнаруживаемые AirMagnet

Название атаки	**Описание**
Airsnarf attack detected	Обнаружены попытки использования утилиты Airsnarf для организации ложных точек доступа и fishing-атак
ARP Request Replay attack	Проводится атака с повтором перехваченного зашифрованного пакета для ускорения вскрытия WEP
Device probing for AP	Клиент настроен на установление соединения с любой точкой доступа
Dictionary attack on EAP methods	Большое количество неудачных попыток установить сессию по протоколу EAP
Faked APs detected	Обнаружено большое количество точек доступа, с которыми не установлено не одного соединения. Это характерно для ситуаций, когда используется утилита FakeAP
Fake DHCP server detected	В беспроводной сети обнаружен сервер DHCP
Hotspotter tool detected	Обнаружены попытки использования утилиты Hotspotter для организации ложных точек доступа и fishing-атак
Illegal 802.11 packets detected	Обнаружен пакет, нарушающий правила стандарта 802.11
Man-in-the middle attack detected	Обнаружена попытка организации атаки «человек посередине»
NetStumbler detected	Обнаружен трафик, характерный для утилиты NetStumbler
Potential ASLEAP attack detected	Обнаружен трафик, характерный для атак на протокол LEAP с использование утилиты ASLEAP
Potential Honey Pot AP detected	Обнаружена точка доступа, маскирующаяся под корпоративную
PSPF violation	Обнаружена прямая передача пакетов между клиентами, что является нарушением политики Publicly Secure Packet Forwarding (PSPF)
Soft AP or Host AP detected	Обнаружено использование программной реализации точки доступа (HostAP, SoftAP)
Spoofed MAC address detected	Обнаружена подмена MAC-адреса, с целью обхода фильтров на основе MAC-адресов
Wellenreiter detected	Обнаружен трафик, характерный для утилиты Wellenreiter

В последнее время в связи с большим количеством обнаруженных уязвимостей в драйверах беспроводных адаптеров в системы WIDS стали включать сигнатуры для подобных атак. Естественно, сигнатуры такого рода не свободны от ошибок первого и второго рода. Например, использование карточки Orinoco 802.11b со стандартными драйверами для Windows приводило к срабатыванию сигнатуры, обнаруживающей заполнение Clear To Send (CTF) пакетами. Инициализация сетевой карточки или переключение ее на другую точку доступа может вызвать обнаружение подмены (spoofing) MAC-адреса. Проблемы могут возникать при использовании злоумышленником нестандартных средств. Например, при использовании программных точек доступа на основе драйвера madwifi, а не HostAP, и «зашумлении» с их помощью эфира ложными фреймами beacon атака может быть не обнаружена.

Механизмы реагирования. Основной задачей системы обнаружения атак является своевременное уведомление администратора о потенциальных проблемах. В беспроводных IDS используются традиционные для систем подобного класса механизмы оповещения, такие как: - отправка сообщения по электронной почте; - уведомление через службу Messenger; - отправка SMS [1;35;36].

Криптоатаки на беспроводные сети с WEP шифрованием. Общие пояснения. Все атаки на WEP основаны на определенных свойствах шифра RC4. Для них всех требуется выполнить перехват пакетов беспроводной сети. В зависимости от типа атаки количество требуемых пакетов различно.

FMS – атака. Атака Fluhrer Mantin Shamir. Является первой предложенной атакой на сети с WEP-шифрованием. Требует, чтобы пакеты содержали “слабые” инициализационные вектора (Weak IV). Требуемое количество перехваченных пакетов от полумиллиона и выше. Сохранять можно только сами IV. При отсутствии “слабых” векторов (например, после коррекции алгоритма шифрования, вследствие “работы над ошибками” разработчика в новой прошивке) атака неэффективна.

Атака KOREK’A. Количество требуемых уникальных IV – несколько сотен тысяч, для ключа длиной 128 бит. Главное требование – чтобы IV не совпадали между собой. Абсолютно не важно наличие слабых IV. Сохранять можно только IV.

PTW – атака. Данный тип атаки позволяет ускорить процесс нахождения WEP-ключа, когда перехватывается большое количество ARP-пакетов. Атака появилась, вследствие появления метода инжекция ARP-запросов в беспроводную сеть. Не использовать подобную возможность было бы глупо. Для криптоанализа требуется сохранять содержимое ВСЕГО перехваченного пакета данных. Количество требуемых пакетов несколько десятков тысяч. На данный момент наиболее эффективная атака.

Единственный минус – почти всегда требуется проводить активную атаку на беспроводную сеть, т.к. ARP-запросы при нормальном функционировании сети никогда не сыпятся как из “рога изобилия”.

Активные атаки. Активные атаки используются для генерации трафика и ускорения сбора данных, необходимых для описанных выше атак. В общем случае они сводятся к инжекции пакетов в беспроводную сеть и генерировании новых IV.

Криптоатаки на беспроводные сети wpa/wpa2. Протокол WPA основан на шифре RC4, который имеет серьёзные недостатки. Протокол WPA2 же основан на стойком шифре AES. В протоколе WPA контроль целостности сообщений (MIC) основан на протоколе Michael. В протоколе WPA2 контроль целостности выполняется с помощью стойкого протокола CCMP. Ход мыслей, я думаю, понятен. Следствием вышесказанного, является то, что WPA может быть теоретически взломан, WPA2 же в теории остаётся стойким. Однако практически реализована пока только атака на аутентификацию WPA/WPA2.

Атаки на wpa-psk/wpa2-psk аутентификацию. Если перехватить этап PSK аутентификации в протоколе WPA или WPA2, то с помощью перебора можно попробовать найти PSK-ключ. Скорость перебора можно увеличить, если заранее вычислить необходимые данные и составить специальные таблицы для перебора. Однако для каждого ESSID будет генерироваться РАЗНЫЕ таблицы, поэтому, не зная заранее (этак за месяцев 5-6 как минимум) ESSID взламываемой точки доступа, чего-то добиться будет сильно проблематично. Но для “стандартных” ESSID (вроде default, linksys) уже существуют вычисленные таблицы. Почему выше, для настроек домашней сети, и рекомендовалось изменять ESSID по умолчанию.

DOS-атаки на беспроводные сети. Существует три варианта DoS-атаки на беспроводную сеть. На физическом уровне модели ISO/OSI (требуется специальное оборудование, например, глушилка). На канальном и выше (требуется обычный беспроводной адаптер). Использующие особенности конкретного оборудования. В первом случае глушится диапазон WiFi (2.4 ГГц), помимо WiFi сетей ещё глушаться все Bluetooth-устройства в радиусе действия. Во втором случае, в зависимости от типа шифрования и аутентификации, будут проводиться специальные действия: деаутентификация клиентов или посылка от их MAC ложных пакетов. В третьем случае используются аппаратные и/или программные уязвимости беспроводных клиентов и/или точки доступа.

3.7. Основные термины, определения и технические характеристики средств защиты информации при утечке информации по электрической сети и цепям заземления

Утечка информации по цепям электропитания. К цепям, имеющим выход за пределы контролируемой зоны и в которые могут проникнуть опасные сигналы через паразитные связи любых видов, относятся, прежде всего, цепи электропитания. Поэтому предотвращение утечки информации по этим цепям является одной из задач инженерно-технической защиты информации [8;21;18;15]. Цепи электропитания обеспечивают передачу электрической энергии в виде переменного электрического тока напряжением 380/220 В и частотой 50 Гц от внешних источников (подстанций) подавляющему большинству устанавливаемых в помещениях радио и электрических приборов. Соединение источника и приемника производят при помощи трех или четырех проводов. При трехпроводной линии передачи источники могут быть соединены как треугольником, так и звездой (рис.32).

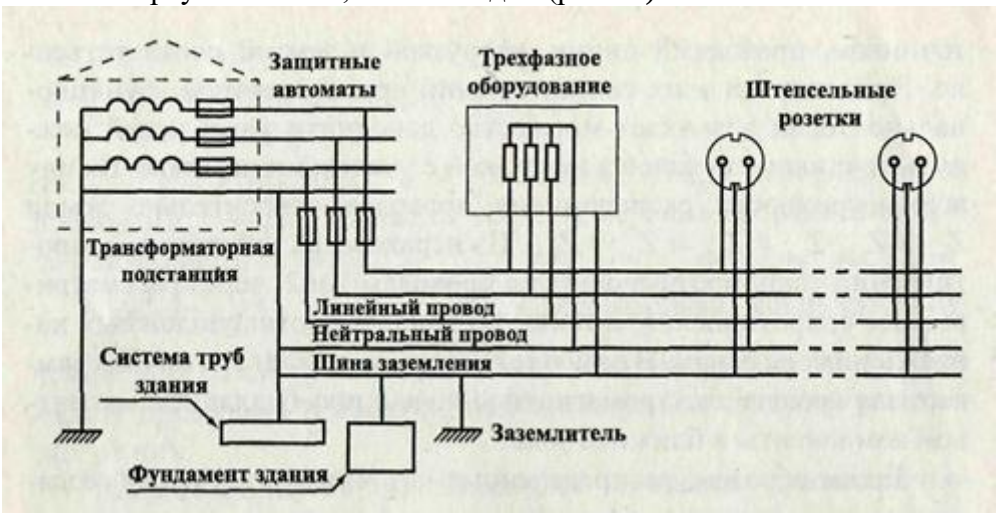


Рис.32. Схема цепей электропитания здания

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

В качестве первичных источников электропитания используются трансформаторные подстанции (ТПС) типа ТП 6-10/04 кВ или другие, понижающие

трехфазное напряжение 6…10 кВ от центрального распределительного пункта (ЦРП) или главной понижающей подстанции (ГПП) до трехфазного напряжения 380 В. К потребителям электроэнергия от трансформаторной подстанции подается, как правило, по радиальной схеме, в соответствии с которой каждый потребитель или их группа питается по отдельной линии от соответствующего коммутационного узла. Линии передачи представляют собой, как правило, четырехжильные силовые кабели [8;21;18;15]. Так как цепи электропитания выходят за пределы охраняемой зоны, то распространение по ним опасных сигналов создает угрозу безопасности защищаемой информации. Существуют, по крайней мере, 4 причины появления опасных сигналов в цепях электропитания [8;21;18;15].

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

Вторая причина обусловлена модуляцией тока электропитания токами радиоэлектронного средства (РЭС). Иллюстрирующая эту причину модель представлена на рис.33.

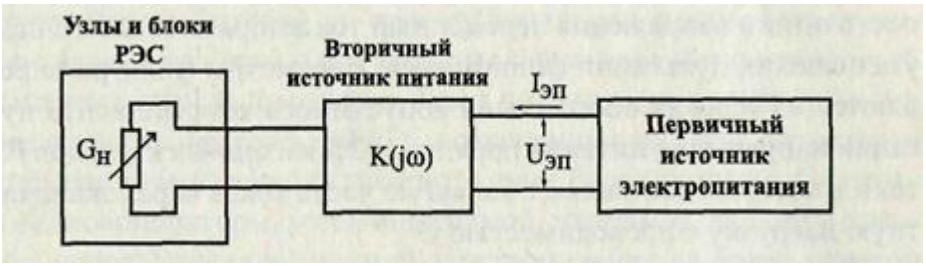


Рис.33. Модель цепи электропитания

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

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

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

Трансформатор преобразует напряжение 220 В в напряжение питания узла (блока) радиоэлектронного средства. Для получения постоянного напряжения

переменный ток выпрямляется и с целью уменьшения пульсаций фильтруется. Параметры фильтра определяются из условия обеспечения допустимого коэффициента пульсаций напряжения питания порядка 1-2% выходных каскадов РЭС, токи в которых составляют большую часть токов через эквивалентную нагрузку с проводимостью G .

Каждый из узлов блока питания оказывает определенное влияние на K(jω). Наибольшие искажения вносят фильтр питания и стабилизатор, которые можно представить в виде фильтра низкой частоты с максимальной частотой пропускания около 30 Гц. Следовательно, типовой вторичный источник питания пропускает от РЭС в цепи электропитания сигналы в диапазоне 0-30 Гц. Если в радиоэлектронном средстве осуществляется обработка (усиление) речевых сигналов, то вторичный источник питания вырезает из его спектра участок шириной до 30 Гц и подавляет спектральные составляющие большей частоты. Учитывая, что спектр речевого сигнала лежит в диапазоне сотен Гц-единиц кГц, вторичный источник питания не пропускает спектральные составляющие речевого сигнала, но пропускает его огибающую. Огибающая речевого сигнала имеет полосу до 60-100 Гц, но его основная энергия сосредоточена в полосе до 30 Гц. Попадание огибающей речевого сигнала в цепи электропитания позволяет при ее перехвате понять смысл сообщения.

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

Четвертая причина вызвана процессами в импульсных блоках питания РЭС, которые применяются вместо традиционных блоков питания с силовыми трансформаторами для частоты 50 Гц. Силовой трансформатор низкой частоты традиционного блока питания имеет большие габариты и вес, которые сдерживают миниатюризацию бытовой и профессиональной радиоаппаратуры. Также велики размеры и вес элементов фильтров (индуктивностей и конденсаторов) выпрямителя блока питания при преобразовании напряжений на частоте 50 Гц. С повышением частоты питающего напряжения уменьшаются габариты и вес блока питания. Поэтому для радиоаппаратуры, устанавливаемой, например, на борту самолетов, используются источники электропитания на более высокой частоте 400 Гц. В современных импульсных блоках питания напряжение 220 В от первичного источника коммутируется электронным ключом, управляемым импульсным генератором с частотой повторения импульсов порядка 100 кГц. Высокочастотное питающее напряжение подается на импульсный трансформатор, выпрямитель, стабилизатор и фильтр блока питания с существенно меньшими габаритами и весом.

Однако высокочастотный ток, протекающий через ключ, имеет сложную форму и, соответственно, широкий спектр. Этот спектр может содержать составляющие, образующиеся в результате комбинаций сигналов импульсного генератора и информационных сигналов, проникающих через паразитные связи из узлов РЭС в элементы блока питания. Высокая частота этих опасных сигналов обеспечивает условия для их излучения в эфир с уровнем, достаточным для обнаружения и приема на удалении нескольких десятков метров [8;21;18;15]. В целях защиты информации от её

утечки по цепям электропитания к системе электропитания объектов информатизации (ОИ) предъявляются определённые требования, к основным из которых относятся следующие [8;21;18;15]:

• электропитание ОИ рекомендуется осуществлять от трансформаторной подстанции, расположенной в пределах контролируемой зоны объекта;

• подключение к распределительному устройству трансформаторной подстанции, питающей объект информатизации, посторонних потребителей, расположенных за пределами контролируемой зоны, должно быть исключено;

• линии электропередачи от подстанции до вводно-распределительного или вводного устройства, установленного в здании, должны прокладываться экранированными (бронированными) кабелями и не должны иметь выходов за пределы контролируемой зоны;

• помещения, в которых установлены распределительные устройства и силовые щиты, а также сами силовые щиты должны закрываться на замки и опечатываться;

• подключение электропитания СВТ, установленных на объекте информатизации, предпочтительно осуществлять от одной фазы или от отдельного щитка. Причём к этой фазе (или щитку) не следует подключать вспомогательные технические средства и системы (ВТСС);

• при совместной прокладке кабелей электропитания СВТ с проводами и кабелями, имеющими выход за пределы контролируемой зоны объекта, расстояние между ними должно быть не менее 0,1 м. При невозможности выполнения этого требования линии электропитания СВТ должны прокладываться экранированными кабелями или в экранированных коробах;

• заземляющие устройства как трансформаторной подстанции, так и объекта информатизации должны находиться в пределах контролируемой зоны объекта не ближе 10 м от её границы;

• все заземляющие проводники должны прокладываться изолированными проводами и кабелями;

• общее сопротивление заземлителя, заземляющих проводников и шин заземления не должно превышать 4 Ом.

При выполнении этих требований в подавляющем большинстве случаев требуемая эффективность защиты информации, обрабатываемой СВТ, от утечки информации по цепям электропитания обеспечивается без применения технических средств защиты информации.

В случаях, если трансформаторная подстанция расположена за пределами контролируемой зоны или к распределительным устройствам, питающим объект информатизации, подключены посторонние потребители, расположенные за пределами контролируемой зоны, для защиты цепей электропитания СВТ должны использоваться технические средства, обеспечивающие фильтрацию опасных сигналов, или системы электромагнитного зашумления.

Утечка информации по цепям заземления. Заземление экранирующих поверхностей способствует ослаблению нежелательных связей и является составной частью системы экранирования. Проводящие поверхности и электрические соединения системы заземления экранов предназначены для протекания обратных токов в сигнальных цепях и цепях электропитания [8;21;18;15].

Одной из причин попадания опасного сигнала в систему заземления является наличие электромагнитного поля — носителя опасного сигнала в местах расположения элементов системы. Это электромагнитное поле будет наводить в расположенной поблизости системе заземления ток опасного сигнала.

Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых контуров заземления. Рассмотрим два устройства, соединенные парой проводников, один из которых является сигнальным, а другой служит для протекания обратных токов (рис.34). Пусть возвратный проводник соединен с корпусом первого (I) устройства, а корпус - с землей. Если этот проводник соединен с корпусом второго (II) устройства, также имеющего электрический контакт с землей (соединение 2'-3'), то образуется замкнутый проводящий контур 2-2'-3'-3-2. Внешнее электромагнитное поле источника опасного сигнала наводит в этом контуре ЭДС, вызывая протекание тока I_{oc}, который, в свою очередь, создает на участке 2-3 падение напряжения U_{oc} (опасного сигнала) равное: $U_{OC} = I_{OC}Z_{23'}$, где Z_{23} — сопротивление участка цепи 2-3.

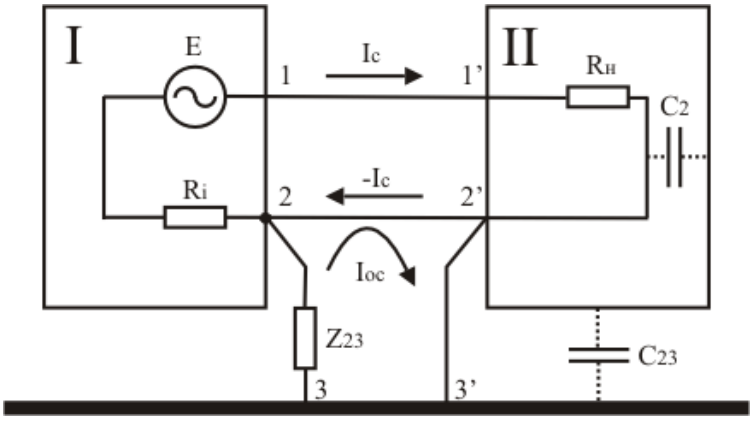


Рис.34. Образование контуров заземления между двумя устройствами

Если отсутствует проводник 2'-3' или соединение проводника 2-2' с корпусом второго устройства, то возможность образования контура заземления полностью не исключается. В этих случаях контур может состоять из проводников 2-2', 3-3', земляной шины и паразитных емкостей между сигнальной цепью и корпусом второго устройства C_2, а также между корпусом второго устройства и землей C_{23}.

Еще одна причина появления опасного сигнала в цепи заземления связана с конечным значением величины сопротивления заземляющих проводников [8;21;18;15]. По заземляющему проводнику протекает обратный электрический ток опасного сигнала (рис.35). Из-за конечного сопротивления $R_з$ земляной шины на этом сопротивлении создается падение напряжения:

$U_{OC} = \frac{U_C R_3}{R_{C1}+R_{C2}+R_3}$, где U_C– напряжение источника сигнала; R_{C1}, R_{C2}— внутреннее сопротивление источника сигнала и сопротивление нагрузки соответственно.

При $R_{C1} + R_{C2} \gg R_3$: $U_{OC} = \frac{U_C R_3}{R_{C1}+R_{C2}}$

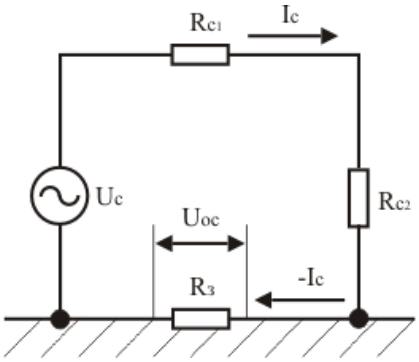


Рис.35. Утечка информации за счет падения напряжения на сопротивлении заземляющего устройства

Напряжение опасного сигнала в цепи заземления будет тем больше, чем больше величина сопротивления R_3.

Утечка информации по цепям заземления может также происходить вследствие того, что общая земля служит обратным проводом для различных контуров. Рассмотрим ситуацию, представленную на рис.36.

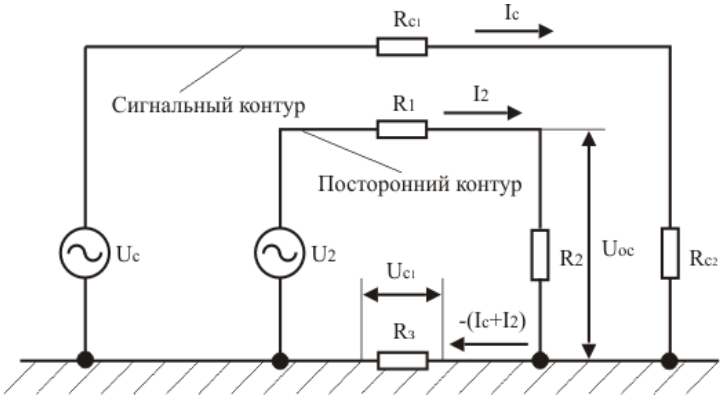


Рис.36. Утечка информации по общей цепи заземления двух различных устройств

В этом случае для двух различных контуров — сигнального и постороннего — общая земля является обратным проводом с эквивалентным сопротивлением R_3.

На эквивалентном сопротивлении земли R_3возникает падение напряжения за счет протекания обратного тока опасного сигнала $-I_c$. На сопротивлении нагрузки R_2 постороннего контура имеет место падение напряжения U_{oc}, вызванное протеканием обратного тока опасного сигнала $-I_c$ по общей цепи заземления, которое равно:

$U_{0C} = \frac{U_{C1}R_2}{R_1+R_2}$, при $R_1 + R_2 \gg R_3$, где R_1 — внутреннее сопротивление источника напряжения U_2 в цепи постороннего контура.

Возможность утечки информации, связанная с цепями заземления, обусловлена также наличием электромагнитного поля опасного сигнала в грунте вокруг заземлителя. Из-за большого затухания, вносимого грунтом, магнитное поле в землю практически не проникает. Электрическое поле в земле определяется величиной потенциала заземлителя и параметрами грунта, где происходит растекание тока

опасного сигнала. С помощью дополнительных заземлителей можно осуществить перехват опасного сигнала (рис.37).

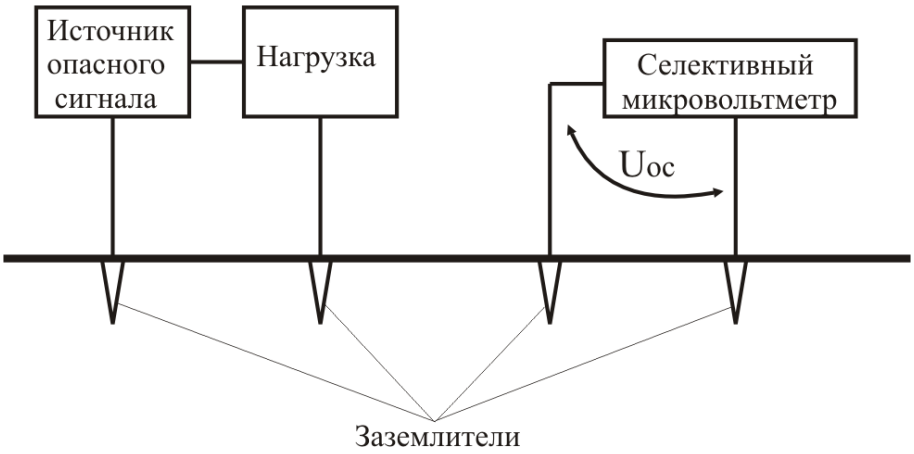


Рис.37. Утечка информации по цепям заземления, обусловленная наличие электромагнитного поля в грунте

Так как цепи заземления выходят за пределы помещения и здания, то распространяющиеся по ним опасные сигналы создают угрозы содержащейся в них информации [8;21;18;15].

Цепи заземления в общем случае создаются для выполнения следующих функций:

- исключение возможности поражения электрическим током персонала, обслуживающего технические средства (защитная функция);
- установление опорного (общего) «нуля» для измерений уровней измеряемых сигналов (базовая функция);
- экранирование электрического поля (экранирующая функция);
- обеспечение путей для протекания возвратных (обратных) питающих и сигнальных токов (возвратная функция).

При заземлении используются два понятия: «земля» и «масса». Под массой понимаются схемотехнические конструкции (шина, провод опорного потенциала, корпус, нулевая точка, нейтрал), по отношению к которым измеряются потенциалы сигналов схемы. «Масса» и «земля», как правило, но не всегда, гальванически связаны друг с другом, а их потенциалы могут отличаться. Потенциал земли, так же как уровень океана, принимается за нулевой. Независимо от выполняемой функции ее эффективность тем выше, чем меньше сопротивление цепи заземления, включающей шину заземления и заземлитель.

Опасные сигналы в цепях заземления возникают по двум причинам:

• наведение в цепях заземления ЭДС полями побочных электромагнитных излучений;

• протекание тока заземления по контуру заземления.

Опасный сигнал может быть «снят» с цепи заземления индуктивным способом или с сопротивления, включенного последовательно в эту цепь. Так как обычно к

одной шине заземления подключается несколько радиоэлектронных средств, то протекающие по ней токи представляют собой смесь токов разных источников. Поэтому выделение в этой смеси опасных сигналов из определенного помещения возможно в принципе, но связано с выполнением ряда условий, в том числе с обеспечением отношения сигнал/помеха, необходимым для выделения информации с требуемым качеством. Помехи представляют собой не только тепловые шумы, но и сигналы других радиоэлектронных средств

Для защиты информации по электромагнитным каналам применяются как общие, так и специальные методы (для данного вида каналов) [8;21;18;15]. Защитные действия можно классифицировать на схемно-конструкторские решения, ориентированные на исключение возможности возникновения таких каналов (рис.38).

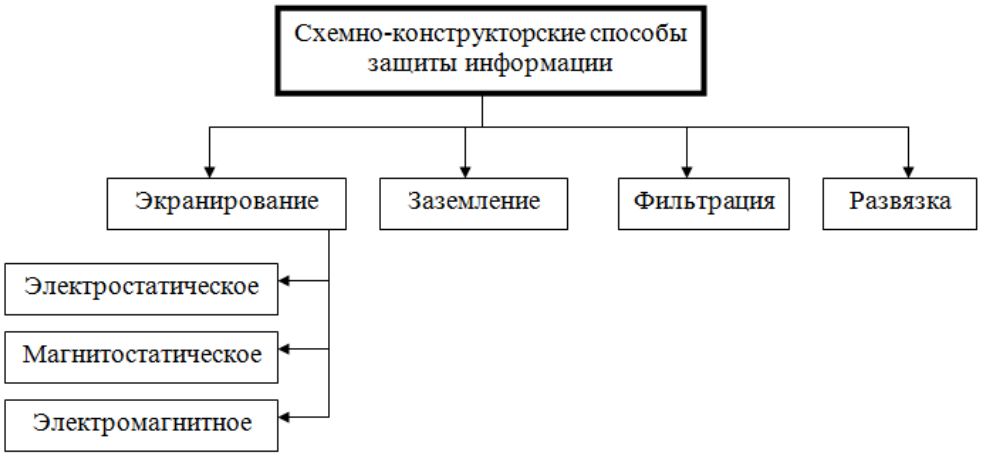


Рис.38. Схемно-технические способы защиты информации от утечки по цепям питания и заземления

Экранирование технических средств. В любом техническом средстве обработки или передачи информации протекают электрические токи различных частот и образуется разность потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля (**побочные электромагнитные излучения**).

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей или последняя много

меньше магнитной за счет свойств излучателя. Переменные электрическое и магнитное поля создаются также в пространстве, окружающем соединительные линии (провода, кабели) ТСПИ. Эффективным методом снижения уровня ПЭМИ является экранирование их источников. Различают следующие способы экранирования: электростатическое; магнитостатическое; электромагнитное [8;21;18;15].

Электростатическое экранирование по существу сводится к замыканию электростатического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля. При использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника наводки в количество раз, равное относительной диэлектрической проницаемости материала экрана.

Эффективность экранирования определяется в основном отношением емкостей связи между источником и рецептором наводки до и после установки заземленного экрана. Поэтому любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования. Экранирующее действие металлического листа существенно зависит от качества соединения экрана с корпусом прибора и частей экрана друг с другом. Особенно важно не иметь соединительных проводов между частями экрана и корпусом. В диапазонах метровых и более коротких длин волн соединительные проводники длиной в несколько сантиметров могут резко ухудшить эффективность экранирования. На еще более коротких волнах дециметрового и сантиметрового диапазонов соединительные проводники и шины между экранами недопустимы. Для получения высокой эффективности экранирования электрического поля здесь необходимо применять непосредственное сплошное соединение отдельных частей экрана друг с другом.

Узкие щели и отверстия в металлическом экране, размеры которых малы по сравнению с длиной волны, практически не ухудшают экранирование электрического поля. С увеличением частоты эффективность экранирования снижается. Основные требования, которые предъявляются к электрическим экранам, можно сформулировать следующим образом:

- конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;

- в области низких частот (при глубине проникновения (δ) больше толщины (d), т.е. при $\delta > d$) эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;

- в области высоких частот (при $d < \delta$) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование используется при необходимости подавить наводки на низких частотах от 0 до 3...10 кГц. Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

- магнитная проницаемость μ_a материала экрана должна быть возможно более

высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);

- увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;

- стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;

- заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов. Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Чем ниже частота, тем слабее действует экран, тем большей толщины приходится его делать для достижения одного и того же экранирующего эффекта. Для высоких частот, начиная с диапазона средних волн, экран из любого металла толщиной 0,5 ... 1,5 мм действует весьма эффективно.

Для частот выше 10 МГц медная и тем более серебряная пленка толщиной более 0,1 мм дает значительный экранирующий эффект. При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

На высоких частотах применяется исключительно **электромагнитное экранирование.** Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления.

Теория и практика показывают, что с точки зрения стоимости материала и простоты изготовления преимущества на стороне экранированного помещения из листовой стали. Однако при применении сетчатого экрана могут значительно упроститься вопросы вентиляции и освещения помещения. В связи с этим сетчатые экраны также находят широкое применение. Необходимая эффективность экрана в зависимости от его назначения и величины уровня излучения ПЭМИН обычно находится в пределах 60... 120 дБ.

Наряду блоками аппаратуры экранированию подлежат и монтажные провода и соединительные линии. Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки должно осуществляться путем непосредственного контакта (лучше всего путем пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания обратного тока.

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой. Экранироваться могут не только отдельные блоки (узлы) аппаратуры и их соединительные линии, но и помещения в

целом. В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующие свойства дверей и окон хуже. Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе:

- токопроводящие лакокрасочные покрытия или токопроводящие обои;
- шторы из металлизированной ткани;
- металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

В помещении экранируются стены, двери и окна. При закрытии двери должен обеспечиваться надежный электрический контакт со стенками помещения (с дверной рамой) по всему периметру не реже чем через 10 ... 15 мм.

Окна должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2х2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя сетки должны иметь хороший электрический контакт со стенками помещения (с рамой) по всему периметру. При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нормальные условия для работающего в нем человека, прежде всего вентиляцию воздуха и освещение.

Заземление. Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений [8;21;18;15]. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

Эта схема наиболее проста, однако, ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

Многоточечная схема заземления практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров. Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5хλ.

На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинированная (гибридная) система заземления, представляющая собой различные сочетания одноточечной,

многоточечной и плавающей заземляющих систем. Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивления заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
- качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;
- контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации и т.д.

Сопротивление заземления определяется главным образом сопротивлением растекания тока в земле. Величину этого сопротивления можно значительно понизить за счет уменьшения переходного сопротивления между заземлителем и почвой путем тщательной очистки перед укладкой поверхности заземлителя и утрамбовкой вокруг него почвы, а также подсыпкой поваренной соли. Таким образом, величина сопротивления заземления будет в основном определяться сопротивлением грунта [8;21;18;15]. Орошение почвы вокруг заземлителей 2 ... 5 процентным соляным раствором значительно (в 5 ... 10 раз) снижает сопротивление заземления.

В таблице 27 приведены экспериментально полученные значения сопротивления заземления стержневого заземлителя (∅15,9 мм, 1 = 1,5 м) для различных грунтов.

Таблица 27

Значения сопротивления заземления стержневого заземлителя (∅15,9 мм, 1 = 1,5 м) для различных грунтов

Тип грунта	Сопротивление заземления $R_З$, Ом		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	14	3,5	41
Глина, суглинки, сланцы	24	2	98
То же с примесями песка	93	6	800
Гравий, песок, камни с небольшим количеством глины или суглинков	554	35	2700

При повышенных требованиях к величине сопротивления заземления (сопротивление заземления ТСПИ не должно превышать 4 Ом) применяют многократное заземление, состоящее из ряда одиночных симметрично расположенных заземлителей, соединенных между собой.

На практике наиболее часто в качестве заземлителей применяют:

- стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
- сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

При необходимости устройства высокочастотного заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления складывается из высокочастотного сопротивления магистрали заземления $Z_З$ (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого заземлителя $Z_З$ (провода, металлического стержня или листа, находящегося в земле).

Величина заземления в основном определяется не сопротивлением заземления, а сопротивлением заземляющей магистрали. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющей магистрали, что достигается за счет уменьшения ее длины и изготовления магистрали в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей магистрали можно сделать весьма небольшой или использовать ее для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно значительно уменьшить величину сопротивления заземлителя $Z_З$. Уменьшить величину $Z_З$ можно также многократным заземлением из симметрично расположенных заземлителей. При этом общее сопротивление заземления будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2 ... 3 м и диаметром 35 ... 50 мм и стальные полосы сечением 50 ... 100 мм. Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее (24 х 4) мм^2.

Магистрали заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания - по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Соединяют магистрали с заземлителем только с помощью сварки. К заземляемому устройству ТСПИ магистраль подключают с помощью болтового соединения в одной точке. При соприкосновении двух металлов в присутствии влаги возникает гальваническая и (или) электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага является электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду.

Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей.

Развязывание информационных сигналов. Принцип изоляции электрической цепи от других цепей в одном устройстве называется гальваническая развязка или изоляция [8;21;18;15]. С помощью такой изоляции осуществляется передача сигнала или энергии от одной электрической цепи к другой, без прямого контакта между цепями.

Гальваническая развязка — передача энергии или сигнала между электрическими цепями без электрического контакта между ними. Гальванические развязки используются для передачи сигналов, для бесконтактного управления и для защиты оборудования и людей от поражения электрическим током. Без использования развязки предельный ток, протекающий между цепями, ограничен только электрическими сопротивлениями, которые обычно относительно малы. В результате возможно протекание выравнивающих токов и других токов, способных повреждать компоненты цепи или поражать людей, прикасающихся к оборудованию, имеющему электрический контакт с цепью. Виды развязывания электрических сигналов в цепях [8;21;18;15]:

- индуктивная развязка (трансформаторы);
- развязка с помощью реле;
- оптроны (оптопары), которые выполнены на основе тиристоров, диодов, транзисторов.

Такой вид гальванической изоляции (оптоэлектронной) обладает некоторыми преимуществами:

• Широкий интервал напряжений развязки (до 0,5 кВ). Это играет большую роль в проектировании систем ввода информации.

• Гальваническая развязка может функционировать с высокой частотой, достигающей нескольких десятков МГц.

• Компоненты схемы такой развязки имеют незначительные габаритные размеры.

При отсутствии гальванической изоляции наибольший ток, который проходит между цепями, может ограничиться только малыми электрическими сопротивлениями.

Фильтрация сигналов. В системах и средствах информатизации и связи фильтрация может осуществляться:

— в высокочастотных трактах передающих и приемных устройств для подавления нежелательных излучений — носителей опасных сигналов и исключения возможности их нежелательного приема;

— в различных сигнальных цепях технических средств для устранения нежелательных связей между устройствами и исключения прохождения сигналов, отличающихся по спектральному составу от полезных сигналов;

— в цепях электропитания, управления, контроля, коммутации технических средств для исключения прохождения опасных сигналов по этим цепям;

— в проводных и кабельных соединительных линиях для защиты от наводок;

— в цепях электрочасофикации, пожарной и охранной сигнализации для исключения прохождения опасных сигналов и воздействия навязываемых высокочастотных колебаний.

Фильтрация в различных цепях осуществляется с помощью фильтров, дросселей и трансформаторов [8;21;18;15]. В целях фильтрации в технических средствах систем информатизации и связи широко используют различные фильтры (нижних и верхних частот полосовые, заграждающие и т.д.). Основное назначение фильтра — пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять сигналы с частотами, лежащими за пределами этой полосы.

Количественно эффективность ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением:

$$\grave{A} = 20\lg\left(\frac{U_1}{U_2}\right) = 10\lg\left(\frac{P_1}{P_2}\right).$$

где $U_1(P_2)$ — напряжение (мощность) опасного сигнала на входе фильтра; $U_2(P_2)$ — напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке. Обобщенная схема фильтрации сигналов представлена на рис.39.

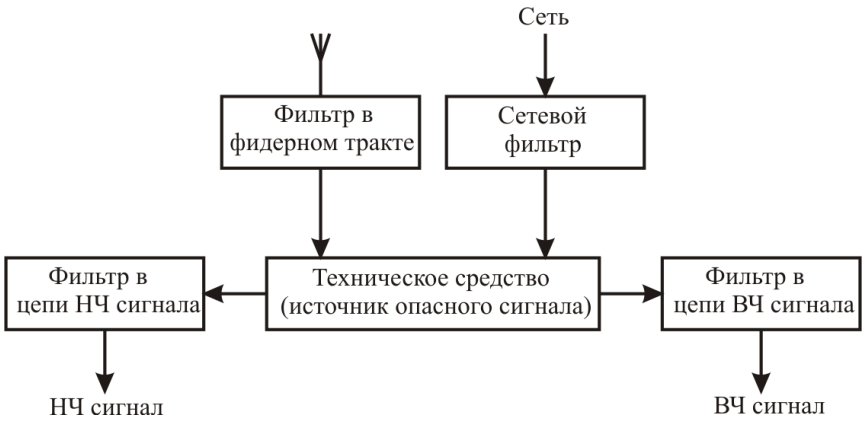


Рис.39. Обобщенная схема фильтрации

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

— величины рабочих напряжения и тока фильтра должны соответствовать величинам напряжения и тока цепи, в которой фильтр установлен;

— эффективность ослабления нежелательных сигналов должна быть не меньше заданной в защищаемом диапазоне частот;

— ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным, не влияющим на качество функционирования системы;

— габариты и масса фильтров должны быть, по возможности, минимальными;

— фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление, удары, вибрация и т.д.);

— конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования [8;21;18;15]:

— затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть незначительным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10^{10} Гц).

— сетевые фильтры должны эффективно работать при больших проходящих токах, высоких напряжениях и высоких уровнях мощности рабочих и подавляемых электромагнитных колебаний;

— ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Фильтры нижних частот. Фильтр, у которого полоса прозрачности находится в пределах от $\omega=0$ (постоянный ток) до некоторой граничной частоты $\omega_{гр}$, называется фильтром нижних частот (ФНЧ).

Фильтры верхних частот. Фильтр, у которого полоса прозрачности занимает все частоты выше некоторой определенной граничной частоты $\omega_{гр}$, называется фильтром верхних частот (ФВЧ). В таком фильтре постоянный ток и все колебания с частотами ниже определенной граничной частоты должны задерживаться, а колебания частот $\omega>\omega_{гр}$ — беспрепятственно пропускаться.

Полосовые и заграждающие (режекторные) фильтры. Полосовые фильтры характеризуются тем, что обе частоты $\omega_{гр1}$, и $\omega_{гр2}$ ограничивающие полосу прозрачности, конечны и ни одна из них не равна нулю.

В ряде случаев ставится задача задержания определенной полосы частот и в то же время пропускания всех остальных частот. Такая задача решается заграждающим фильтром.

С точки зрения конструктивного исполнения фильтры могут быть выполнены на элементах с сосредоточенными параметрами (фильтры, предназначенные для работы на частотах до 300 МГц) и на элементах с распределенными параметрами (коаксиальные, волноводные, полосковые, применяемые на частотах свыше 1 ГГц). В

диапазоне частот 300 МГц-1 ГГц могут использоваться фильтры, включающие элементы, как с сосредоточенными, так и с распределенными параметрами.

Разделительные трансформаторы. Должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки [8;21;18;15]. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

— разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;

— устранения асимметричных наводок;

— ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем: - величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи; - величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой; - ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным; - габариты и масса фильтров должны быть минимальными; - фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.); - конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования [8;21;18;15]: - затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц); - сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний; - ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное

значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания, но не более их.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это может привести к тому, что: - ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр; - возникает взаимозависимость переходных процессов в различных нагрузках цепи питания. Наибольшие скачки напряжения при этом возникают во время отключения нагрузок, так как большинство из них имеет индуктивный характер. Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, а LC-фильтр из десяти или более элементов - более 200 дБ/декада. Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40 ... 60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать экранированные фильтры с разъемами и использовать для соединения экранированные провода. Фильтры с гарантируемым затуханием 100 дБ выполняют в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей. Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (f_c) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад [8;21;18;15].

Частотный диапазон фильтров типа ФП от 0,15 до 1000 МГц. Ориентировочные значения максимального затухания для сетевых фильтров, приведены в таблице 28. Основные характеристики помехоподавляющих фильтров приведены в таблице 29.

Таблица 28

Значения максимального затухания для сетевых фильтров

Диапазон частот	Максимальное затухание фильтра вне полосы пропускания, дБ		
	экранированный		неэкранированный
	с разъемами	без разъемов	
Фильтры в цепях питания на токи не более 10 А			
$f_c \le f \le 10\ f_c$	80	-	-
$10\ f_c \le f \le 100\ f_c$	80	-	-
$f > 100\ f_c$	70	-	-
Фильтры в цепях питания на токи более 10 А			
$f_c \le f \le 10\ f_c$	100	-	-
$10\ f_c \le f \le 100\ f_c$	100	-	-
$f > 100\ f_c$	90	-	-

Например, фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток - от 2,5 до 70 А.

Таблица 29

Основные характеристики помехоподавляющих фильтров

Наименование характеристик	**Тип фильтра**					
	ФП-1	**ФП-2**	**ФП-3**	**ФП-4**	**ФП-5**	**ФП-6**
Количество проводов	2	2	2	2	2	2
Номинальный ток, А	24	40	40	40	10	20
Номинальное напряжение (фаза-земля), В						
- постоянного тока	500	250	500	1000	500	500
- переменного тока 50 Гц	220	110	220	500	220	200
- переменного тока 400 Гц	110	60	110	220	110	110
Вносимое затухание, дБ	60					

Наименование характеристик	**Тип фильтра**								
	ФП-7	**ФП-8**	**ФП-9**	**ФП-10**	**ФП-11**	**ФП-12**	**ФП-13**	**ФП-14**	**ФП-15**
Количество проводов	2	2	2	2	2	2	2	2	4
Номинальный ток, А	1,0	2,5	4,0	10,0	16,0	20,0	20,0	40,0	70,0
Номинальное напряжение (фаза-земля), В									
- постоянного тока	250	1000	1000	500	1000	500	1000	1000	500
- переменного тока 50 Гц	110	500	380	220	380	220	500	500	220
- переменного тока 400 Гц	60	220	110	110	110	110	220	220	110

Фильтры серии ФСПК-100 (200) [18;15] предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ.

Характеристики фильтров. К характеристикам фильтров относятся [10;18;15]:

1) передаточная функция;

2) амплитудно-частотная характеристика;

3) фазо-частотная характеристика;

4) частота среза ωср (fср);

5) постоянная времени τ;

6) полоса пропускания (подавления) Δω (Δf);

7) резонансная частота;

8) добротность *Q*.

Передаточная функция фильтра это отношение изображения по Лапласу выходной величины изображению по Лапласу входной величины фильтра.

$K(p) = \frac{L\{U_{\text{ВЫХ}}(t)\}}{L\{U_{\text{ВХ}}(t)\}}$. В общем случае фильтр можно рассматривать как четырехполюсник с передаточной функцией

$K(p) = \frac{U_2(p)}{U_1(p)} = \frac{a_m p^m + a_{m-1} p^{m-1} + \cdots + a_1 p + a_0}{b_n p^n + b_{n-1} p^{n-1} + \cdots + b_1 p + b_0}$, где $U_1(p)$ $U_2(p)$ – входное и выходное напряжение четырехполюсника в операторной форме; a и b – вещественные постоянные величины; m, n = 1,2,3, …; n – определяет порядок фильтра.

Для установившейся частоты p = jω и передаточную функцию можно привести к виду

$$K(p) = \frac{U_2(j\varpi)}{U_1(j\varpi)} = \frac{a_m(j\varpi)^m + a_{m-1}(j\varpi)^{m-1} + \cdots + a_1(j\varpi) + a_0}{b_n(j\varpi)^n + b_{n-1}p(j\varpi)^{n-1} + \cdots + b_1(j\varpi) + b_0} = A(\varpi) + jB(\varpi)$$

Модуль передаточной функции называется *амплитудно-частотной* характеристикой $|K(j\varpi)| = \sqrt{A^2(\varpi) + B^2(\varpi)}$

Фазо-частотная характеристика также может быть представлена в виде

$\varphi(\varpi) = arctg(\frac{B(\varpi)}{A(\varpi)})$. Диапазон Δω = ω2–ω1 или полосы частот, в которых проходят сигналы, называются *полосами пропускания*. В полосе пропускания значение коэффициента передачи фильтра относительно велико, а в идеальном случае постоянно. Для полосового фильтра частоты ω1 и ω2 (рисунок 40, в), определяются при спаде коэффициента передачи на 3 дБ.

Диапазон частот Δω = ω2 –ω1 (рисунок 40, г), в которых сигналы подавляются, образуют *полосу задержания*. В полосе задержания коэффициент передачи фильтра относительно мал, а в идеальном случае равен нулю. Для заграждающего фильтра частоты ω 1 и ω 2 определяются при спаде коэффициента передачи на 3 дБ.

Частота среза ω_{CP} (fcp) – частота на которой наблюдается спад коэффициента передачи на 3 дБ по сравнению с коэффициентом передачи на нулевой (для ФНЧ) или бесконечной (для ФВЧ) частоте.

Резонансная частота f_P – частота, на которой коэффициент передачи фильтра имеет максимальное значение (для полосового фильтра) или минимальное значение (для заграждающего фильтра).

Добротность Q - добротность полосового фильтра определяется как отношение резонансной частоты к полосе пропускания $Q = f_P/(\varpi_2 - \varpi_1)$. Амплитудно-частотные характеристики (АЧХ) различных фильтров представлены на рис.40.

Фильтр нижних частот пропускает низкие частоты и задерживает высокие (рисунок 40, а), фильтр верхних частот задерживает низкие частоты и пропускает высокие (рисунок 40, б), полосовой фильтр пропускает полосу частот от ω1 до ω2 и задерживает те частоты, которые расположены выше или ниже этой полосы частот (рисунок 40, в), режекторный фильтр задерживает полосу частот от ω1 до ω2 пропуская частоты, расположенные выше или ниже этой полосы частот (рисунок 40, г).

В указанных фильтрах коэффициент передачи и фазовый сдвиг зависят от частоты входного сигнала. Фильтры, у которых коэффициент передачи остается постоянным, а фазовый сдвиг зависит от частоты, называются фазовыми фильтрами.

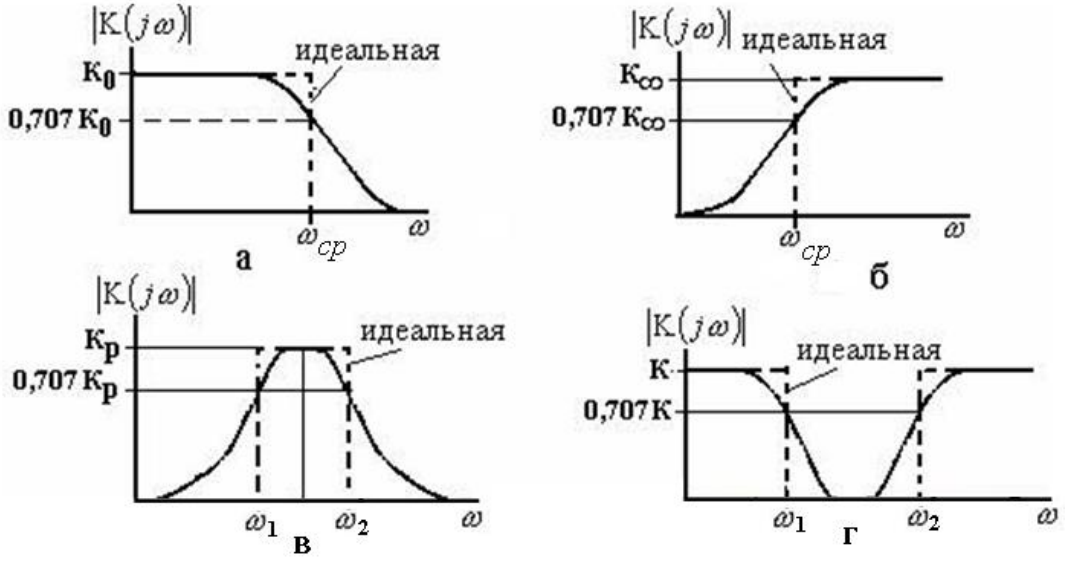


Рис.40. АЧХ фильтров

В зависимости от аппроксимирующего полинома фильтры разделяются на фильтры критического затухания, Бесселя, Баттерворта, Чебышева. При изложении принципа построения аппроксимирующих функций фильтров как основу обычно используют ФНЧ. На рис.41 показаны АЧХ указанных фильтров нижних частот.

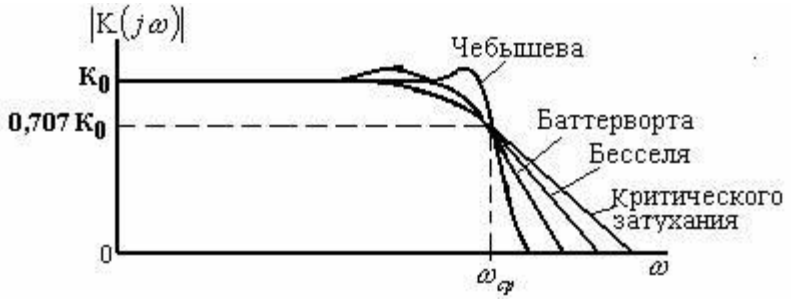
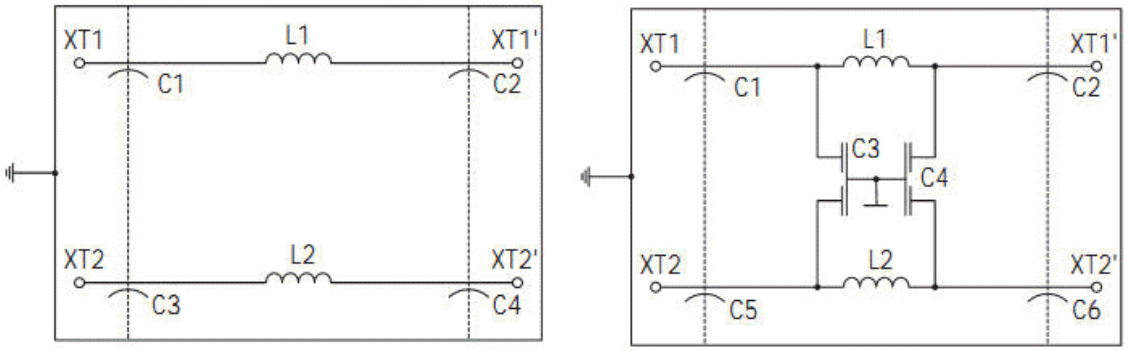


Рис.41. Характеристики фильтров в зависимости от аппроксимирующего полинома

АЧХ ФНЧ Баттерворта имеет довольно длинный горизонтальный участок и резко спадает за частотой среза. Переходная характеристика такого фильтра при ступенчатом входном сигнале имеет колебательный характер. С увеличением порядка фильтра колебания усиливаются. Характеристика фильтра Чебышева спадает более круто за частотой среза. В полосе пропускания она имеет волнообразный характер с постоянной амплитудой. Колебания переходного процесса при ступенчатом входном

сигнале сильнее, чем у фильтра Баттерворта. Фильтр Бесселя характеризуется меньшей длиной горизонтального участка, чем фильтр Баттеворта и более пологим спадом АЧХ за частотой среза, чем фильтры Баттерворта и Чебышева. Данный фильтр обладает оптимальной переходной характеристикой (переходный процесс практически не имеет колебаний). Фильтр критического затухания обладает значительно худшей амплитудно-частотной характеристикой по сравнению с фильтром Бесселя, но не имеет перерегулирования. В общем фильтр критического затухания уступает фильтру Бесселя в отношении качества отработки входного ступенчатого сигнала [10;18;15]. Примеры схем фильтров в полосе частот от 150 кГц до 1000 МГц представлены на рис.42.



а) б)

Рис.42. Принципиальная схема помехоподавляющего фильтра, обеспечивающего эффективность фильтрации опасных сигналов в полосе частот от 150 кГц до 1000 МГц не менее 60 дБ (а) и 80 дБ (б)

При установке фильтров на объектах информатизации должны быть выполнены следующие требования и рекомендации [10;18;15]: - четырёхпроводные помехоподавляющие фильтры («объектовые фильтры») необходимо устанавливать на кабели, питающие группы СВТ, как можно ближе к питающим трансформаторам в пределах контролируемой зоны. Целесообразно их устанавливать в специальных помещениях или металлических шкафах, закрываемых на ключ; - двух и трёхпроводные сетевые помехоподавляющие фильтры, предназначенные для питания отдельных СВТ, («фильтры для локальных цепей»), должны устанавливаться внутри помещений (объектов информатизации) и монтироваться таким образом, чтобы исключить возможность появления наведённого сигнала в фильтруемых (отходящих от фильтра) проводах электропитания. Это требование выполняется, если фильтр будет удалён от СВТ на расстоянии не менее, чем r1; - корпус фильтра должен быть заземлён на контур рабочего заземления, заземлитель которого должен находиться в пределах контролируемой зоны на расстоянии не менее 10 м от её границы.

Проходные конденсаторы в фильтрах. Для защиты от помех, которые могут проникнуть в прибор через цепи питания и наоборот, а также для различных блокировок используют так называемые **проходные конденсаторы** [10;18;15]. Такой конденсатор имеет три вывода, два из которых представляют собой сплошной токонесущий стержень, проходящий через корпус конденсатора. К этому стержню присоединена одна из обкладок конденсатора. Третьим выводом является металлический корпус, с которым соединена вторая обкладка. Корпус проходного конденсатора закрепляют непосредственно на шасси или экране, а токоподводящий провод (цепь питания) припаивают к его среднему выводу. Благодаря такой конструкции токи высокой частоты замыкаются на шасси или экран устройства, в то время как постоянные токи проходят беспрепятственно. Проходной конденсатор - конденсатор, предназначенный для использования в цепях питания, служит простейшим С-фильтром, развязывающим по высокой частоте источники питания от нагрузки. Их назначение - отводить высокочастотную составляющую (помеху) на землю. Конструктивно устанавливается между двумя взаимно-экранированными блоками. На высоких частотах применяют **керамические проходные конденсаторы**, в которых роль одной из обкладок играет сам центральный проводник, а другой — слой металлизации, нанесенный на керамическую трубку. Эти особенности конструкции отражает и условное графическое обозначение проходного конденсатора (рис.43).

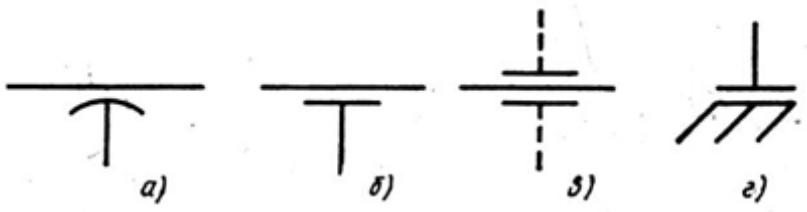


Рис.43. Изображение на схемах проходных и опорных конденсаторов.

Наружную обкладку обозначают либо в виде короткой дуги (а), либо в виде одного (б) или двух (в) отрезков прямых линий с выводами от середины. Последнее обозначение используют при изображении проходного конденсатора в стенке экрана.

Контрольные вопросы:

- Дайте общую классификацию каналов утечки информации, обрабатываемой техническими средствами обработки информации;
- Классификация акустических каналов утечки информации;
- Классификация каналов скрытого видеонаблюдения и съемки;
- Классификация ТСЗИ от утечки по техническим каналам;

- Классификация программных СЗИ от утечки по техническим каналам;
- Опишите общие физические характеристики акустических сигналов;
- Звукоизоляция и виброизоляция помещений и типовые характеристики звукоизоляции строительных конструкций;
- Классификация микрофонов;
- Технические характеристики микрофонов;
- Классификация и схемы образования опасных сигналов;
- Понятия контролируемой зоны, зон R1 и R2, зон r1 (r1');
- Виды акустоэлектрических преобразований, низкочастотных и высокочастотных излучений технических средств;
- Паразитные связи и наводки в технических средствах;
- Классификация акустических радиопередающий закладных устройств;
- ВЧ навязывание, методы ВЧ навязывания;
- Пассивные и полуактивные радиозакладные устройства;
- Основные технические характеристики радиоприемной и радиопередающей аппаратуры;
- Основные технические характеристики радиосканеров и пеленгаторов;
- Классификация и технические характеристики антенно-фидерных устройств;
- Классификация утечек информации в проводных линиях связи;
- Классификация телефонных закладок;
- Основные способы защиты телефонных линий;
- Характеристики оборудования защиты в проводных линиях связи;
- A8 - алгоритм генерации ключа в сетях мобильной связи;
- Типы и алгоритмы работы поточных шифров в сетях мобильной связи. ШИФР RC4. ШИФР SEAL. ШИФР VMPC. ШИФР TRIVIUM.
- Виды и классификация беспроводных сетей. Персональные беспроводные сети стандарта 802.11.
- Сети WiMAX и сети Wi-Fi. Спецификация по протоколу стандарта 802.11;
- Типовые протоколы безопасности Wi-Fi и меры защиты для Wi-Fi;
- Основные положения политики безопасности беспроводных сетей;
- Механизмы защиты технологии Bluetooth;
- Атаки на пользователей WLAN;
- Криптоатаки на беспроводные сети с WEP шифрованием;
- Утечка информации по цепям электропитания;
- Утечка информации по цепям заземления;
- Экранирование технических средств, типы экранирования;
- Заземление технических средств, требования к средствам заземления;
-Развязывание и фильтрация информационных сигналов;
- Технические характеристики фильтров.

Приложение 1. Сводная таблица характеристик акустических устройств несанкционированного съема информации

№ п/п	Наименование (марка)	Частота мГц	Вид модуляции	Выход мощность мВт	Диапазон НЧ сигнала Гц	Размеры, мм	Питание, В	Прочие примечания
Акустические радиозакладные устройства								
1	SIM-F35-TX	410-424	FSK	25/50/95	200-6000		3,5-12	Скорость прд. 100кб/с, динамический НЧ-диапазон 89 дБ
2	SIM-A-62	130-80 (350-480)	NFM (10 кГц)	5-30		8x6x28	DC 1,4-4,5	Внутренний или внешний микрофон МОП - технология
3	SIM-A-13TL	200-250 (136-174)	FM (±15кГц)	5-20		45x31x9	DC 5-12,5	Дист. управление, кодирование информации, время работы 40 ч
4	SIM-A-31	10,5 ГГц	WFM	30		40x27x13	DC 8-14	Дист. управление
5	COF-33S	890 -980	BPSK (ΔF - 8МГц)	10/100	40-16000	78x48x11	DC 9	
6	SIM -DSS -5000	850-950/ 750-850	BPSK (ΔF 10МГц)	3 - 300 (регулир)	150-7000 VOX	94x57x11	DC 6	ППРЧ в диапазоне 100 МГц, динамический НЧ-диапазон 70 дБ
7	PK 1945-SS	UHF	DTWF	50		46x37x17	DC 9	ППРЧ (период 0,5-3 с)
8	SIM - PR-9000T	350 -450	BPS (ΔF - 5МГц)	100		70x39x5	DC 6-10	Двухкан. режим, кодирование информации
9	SIM DSS-2000	850-952/ 400-450	BPS (ΔF - 16МГц)	10 - 1000 (регулир)	150-7000 VOX	83x53x19	DC 6 (внешнее)	Дист. управление включ. и мощ прд., кодирование информации
10	Omega 1	305-365	ВИМ	10-200	50-5000	41x17x7	DC 4-12	Дист. управление
11	X-3	87-108	WFM (±75кГц)	дальность 400-500м		28x18x11	1,5	Время работы от батареи 100ч
12	HKG 2015-A	85-110/ 130-150	FM	дальность 500м		73x65x19	2xZM-9	Дист. управление, время работы от батареи 1500ч
13	HKG 2018	88-110/ 130-150	FM	50		853x65x20	9	Время работы от батареи 50ч
14	RM-02M	88-115/ 130-150	WFM	дальность 150-300м		29x19x12	1,5	Время работы от батареи 150ч
15	Авто - 417	415-435	WFM	дальность 750м		30x20x8	12,5 (внешнее)	Кварцевая стабил частоты

Продолжение приложения 1

№ п/п	Наименование (марка)	Частота мГц	Вид модуляции	Выход мощность мВт	Диапазон НЧ сигнала Гц	Размеры, мм	Питание, В	Прочие примечания
16	НЛ-417 КИ	415-425	FM	дальность 400м				Кварцевая стабил частоты кодирование информации
17	HKG-2000	88-110/ 130-150	FM	дальность 1000м		59x39x17	9	Время работы от батареи 100/250ч
18	HKG-2007 (фломастер)	88-110/ 130-170	FM	дальность 200м		d12x135	5x1,5	
19	HKG-2062 (калькулятор)	88-110/ 130-170	FM	дальность 300м				
20	PRO 470 R/M	470	WFM	дальность 100-150м		30x10x5	СЦ-18	Время работы от батареи 50ч
21	Таблетка-450	450-455	WFM	дальность 100м		30x7		Время работы от батареи 50ч
22	HKG-2009 (удлинитель)	130-170/ 88-110	FM	дальность 250м		150x57x40	220В	
23	HKG-2005 (зажигалка)	130-170/ 88-110	FM	дальность 150м		85x53x32	9В	Время работы от батареи 120ч
24	Sheaffer (авторучка)	110-115/ 130-150	WFM	дальность 200м		15x130	1,5	Время работы от батареи 8ч
25	VIC 711-DT	430,25-479,25 (шаг 10 кГц)	FSK	100 - 800 (управл)		40x17x6	9-10	Дист. управление, в т.ч. мощностью прд
26	Inca Board TXF RC	UHF320-330; U4:440- 450	NFM (± 3 кГц)	UHF: 60; U4: 50	100-5000	110x45x8	3,7	Дист. управление
27	SIM-SAW-13	293 - 325	WFM	1	100-7000	29x7x4	3(CR2450)	
28	SIM-SAW-16	640 - 680	WFM	1	100-7000	29x7x4	3(CR2450)	
29	SIM-SAW-106	640 - 680	WFM	10	100-7000	29x7x4	3(CR2450)	Стабилизация частоты
30	UHF-STE batteria	416,5 - 423	WFM	5-7	200-6000	d30x18	lxCR 2450	вид исполнения — «таблетка»; время работы от батареи 48ч

Окончание приложения 1

№ п/п	Наименование (марка)	Частота мГц	Вид модуляции	Выход мощность мВт	Диапазон НЧ сигнала Гц	Размеры, мм	Питание, В	Прочие примечания
Радиозакладные устройства с промежуточным накоплением информации								
31	INCA ULL	440-450/ 320-330/ 150-175-	FM	50; 60; 80	100-5000	70x41x20	DC 4-15	Дист. управление, время накопления 12/24ч
32	SIM-BURST	800-1200	GMSK	40-400 (управл)	150-7000	155x30x10	DC 3,6-4,6	Дист. управление, время передачи 20-250мс
Акустические закладные устройства с передачей информации по инфракрасному каналу								
33	HKG-1830	Ближний ИК		дальность 300-700м		45x30x18	DC 6	время работы от батареи 20ч
34	SIM IR100	Ближний ИК		дальность 200м		d13x31	DC 2-3	
35	RK-775	0,93 мкм длина волны			100-8000	44x30x17	DC 6	время работы от батареи 15ч
36	RKI-3200	0,87 мкм длина волны	NFM	40		45x35x15	DC 6	
37	STG IRTX	0,88 мкм длина волны		дальность до 500м	200-3000	66x27x14	2x1,5	
38	4500-IRTX	0,88 мкм длина волны		дальность до 500м	200-3000	66x27x14	2x1,5	
Акустические закладные устройства с передачей информации по сети 220В (сетевые закладки)								
39	РК 1295-SS	200-400 кГц	NFM (±6 кГц)			60x40x16	220В	Скачкообразное изм. частоты. Потр. мощность 100 мВт
40	РК 1295-S	60-200 кГц	NFM (±6 кГц				220В	
41	СОР 260	193 кГц	FM		300-3000	85x58x36		Выходная мощность передатчика 3 Вт
42	HKG-2221	120-260 кГц	FM			67x35x25		6 каналов. Дальность передачи до100 м

Приложение 2. Сводная таблица характеристик акустических полуактивных устройств несанкционированного съема информации

№ п/п	Наименование (марка)	Частота облучения мГц / Вид модуляции	Частота переизлучения мГц	Мощность облучения Вт / Мощность переизлучения мВт	Дальность, м	Размеры, мм	Питание, В / время работы	Прочие примечания
1	81М-ЛТР-16	160	160+0,012	10 / -	500	90х90х4	- /2000-4000	аудиотранспондер
2	81М-ЛТР-40	800-950		0,1-20 мВт /	500	130х75х250	3В/ 4 месяца	аудиотранспондер
3	SIPE MM1				100	d25x300	-	Пассивная закладка
4	SIM - ATP -16	160 / NFM	160,012	10 Вт	50 ... 300	90х90х4	- /2000-4000	Аудиотранспондер, диапазон звукового сигнала – 75 ... 10000 Гц
5	PK - 500				10		-/ 10лет	Пассивная закладка
6	SIM - TR - 40	800-950/ NFM	800-950	0,1-20 мВт	50 ... 300	6х25	3В/ 4 месяца	Аудиотранспондер, диапазон звукового сигнала – 75 ... 10000 Гц

Приложение 3. Сводная таблица характеристик направленных микрофонов

№ п/п	Наименование (марка)	Частота приема, Гц	Коэффициент усиления, дБ	Дальность, м	Чувствительность мВ/Па	Размеры, мм	Питание, В / время работы, ч	Прочие примечания
Трубчатые микрофоны								
1	AT4071A	30-20000			89,1	395x21x21		
2	МКН70 Р48	50-20000			50	410x25x25		
3	KMR82i	20-20000			21	395x21x21		
4	MFC800	20-20000			18	500x25x250		
5	YKN	500 – 10 000	66	100	20	310x30	3 / 30	
6	AT-89	60 – 12 000	93	100	70	355x70	9 / 4-6	
7	UEM-88	200 – 15 000	50			229x25x13	1,5 / 100	
8	МД-74	10 - 10000			1,2	71x810		
9	КМС-19-05	20-20000			45	24x850		
10	КМС-1909	20-20000			30	24x203		
11	МКЕ-802	50-15000			13	22x292		
Параболические микрофоны								
№ п/п	Наименование (марка)	Частота приема, Гц	Коэффициент усиления, дБ	Дальность, м	Чувствительность мВ/Па	Диаметр отражателя (размеры) мм	Питание, В / время работы, ч	Прочие примечания
1	Big Easer BE3K	100-15000			31	500x500x400		
2	Spectra G50	100-15000			50	750x750x400		
3	PKI 2920			150		850	9 аккум	
4	PKI 2915			100		600	9 аккум	
5	Super Sound Zoom	500-14000			4	290x150x90		
6	PR 1000	200-14000			20	500x500x400		
7	Супер Ухо 100	100 -14000	До 70	50-100		290 x 150 x 90	9 / 60	
8	Супер Ухо SD	100 -14000	До 70	50-100		290 x 150 x 90	9 / 60	с записью за SD карту памяти до 10 часов
9	AA79100			150		d600		

Окончание приложения 3

№ п/п	Наименование (марка)	Частота приема, Гц	Динамический диапазон, дБа	Дальность, м	Чувствительность мВ/Па	Размеры решетки мм	Кол-во микрофонов	Прочие примечания
Микрофонные решетки								
1	SPT980	20-20000	20-135		50	d1000	36	Microphone Model MPA231T
2	SPS980	20-20000	30-128		50	d1000	36	Microphone Model MPA231T
3	SPS490	20-20000	30-128			d500	16	Microphone Model MPA416
4	40TA	50-6600	32-134		50	175x175	64	

Приложение 4. Сводная таблица характеристик лазерных микрофонов

№ п/п	Наименование (марка)	Тип лазера	Длина волны мкм / фокусное расстояние, мм	Мощность излучения, мВт	Дальность, м	Питание, В	Время работы, ч	Прочие примечания
1	SIM LAS-MIC	полупровод	0,82 / 135	5		8x1,5	50	
2	Laser - 3000	полупровод	0,88 / 135	10		4x1,5	50	До 100 дБ усиление
3	Laser - 2000	полупровод	0,75-0,84 / 135	5		8x1,5	50	
4	Laser - 3500	полупровод	1,75-1,84 / 135	5		8x1,5	40	
5	MR - 7800	полупровод	0,77-0,84 / 135	25		8x1,5	40	
6	AA79106-B	полупровод	/ 135					
7	HP-150	гелий-неонов	0,63 /		500-1000			фирмы "Hewlett-Packard"
8	RA79107CH	полупровод	0,88 / 135	20	До 500	4x1,5	50	

Приложение 5. Сводная таблица характеристик электронных стетоскопов

№ п/п	Наименование (марка)	Коэф-нт Усиления, дБ	Тип микрофона	Толщина стен прослушивания разговоров, м	Полоса частот, Гц вибродатчика	Размеры, мм	Питание, В /Время работы, ч	Прочие примечания
1	RKI 2900	100	пьезомикрофон		150-4800	d20x35	9 / 20	
2	UM 012			до 0,5	150-3500			высокочувствительный вибромикрофон
3	Изделия фирмы DTI			до 1	300-3000			
4	UM121			до 1	300-3000			
5	РК-915		пьезомикрофон			d20 x 15	1,5	Встроенный усилитель. Время работы – 500 ч. Длина провода - 0,5 м
6	РК-815-S	20 000	контактный	до 0,5		d4 x 14	9	Время работы – 80 ч
7	РК-845-SS	25 000	Электретный	до 0,7		8 x 1,5		Время работы - 120 часов. Длина провода – до 500 м.
8	НВ - 04	100	пьезомикрофон	до 0,5		d30 x 25	9	Время работы не менее 40 ч Длина кабеля - до 25 м.
9	HKG - 2038 A	100	контактный	до 0,5		d6 x 6	9	Время работы 250 часов. Длина кабеля - 50 м
Электронные радиостетоскопы								
№ п/п	Наименование (марка)	Частота, Гц / Вид модуляции	Выходная мощность, мВт	Толщина стен прослушивания разговоров, м	Дальность действия, м	Размеры, мм	Питание, В /Время работы, ч	Прочие примечания
1	UM 006	108-112,5		до 0,5				
2	Радиозакладка SIPE RS			до 0,5	до 250			
3	HKG - 2039	88...110; (130...150) / FM			1 000	85 x 65 x 20	9 / 100	Электретный микрофон

Продолжение приложения 5

№ п/п	Наименование (марка)	Частота, Гц / Вид модуляции	Выходная мощность, мВт	Толщина стен прослушивания разговоров, м	Дальность действия, м	Размеры, мм	Питание, В /Время работы, ч	Прочие примечания
4	4025-STTX	115 ... 150 / WFM	3	до 0,5		22 х 22 х 14	2х1,5	
5	HKG - 2039	130...150; (88...110) / WFM			1000	85х65х20	9 /100	Электретный микрофон
6	РК - 1005	130...175 (1,3 ГГц) / WFM (± 50 кГц)	6			30х30х20	3 / 48	
7	4026 (4027)-STTX	135...170 (380...440) / NFM	5	до 0,5		45х30х20	6 /	Кварцевая стабилизация частоты
8	МС-02	96-108 (регулируемая)			700	50Х20	9 /	
9	РК - 1005-S	VHF (A, B, C) / NFM (± 5 кГц)	40			45х30х15	9 /	Кварцевая стабилизация частоты
10	HKG - 1132	VHF / NFM (± 3 кГц)	20	до 0,4	400 ...1 000	59х30х18	2х3,4 /	Кварцевая стабилизация частоты
11	РСБ - 417 К (таблетка)	415 ... 420 / WFM		до 0,4	150	34х23	CR 2425 / 60	
12	РМ - СТ	415 ... 430 / FM	45	до 0,4		58х38х18	9 / 48	
13	ГСТ-радиостетоскоп	429 / WFM	5		150	33х33х23	CR2450 / 30	Кварцевая стабилизация частоты
14	Кирпич Ст	430 ... 470 / FM			500		/ 10 лет	Кварцевая стабилизация частоты. Дист. управление.
15	П - 475	470 ... 475 / WFM		до 0,3	100	40х28	2 • РЦ-53 / 30	Кварцевая стабилизация частоты
16	HKG - 1131	UHF / NFM (± 3 кГц)	20		400-1000	45х30х18	6 /	Кварцевая стабилизация частоты

Окончание приложения 5

№ п/п	Наименование (марка)	Частота, Гц / Вид модуляции	Выходная мощность, мВт	Толщина стен прослушивания разговоров, м	Дальность действия, м	Размеры, мм	Питание, В /Время работы, ч	Прочие примечания
17	PK - 1005-SS	UHF (A,B,C) / NFM (± 5 кГц)	20			45x30x15	9 /	Кварцевая стабилизация частоты
18	HKG - 1133	SHF (ГГц) / NFM (± 3 кГц)	20		400-1000	59x30x18	2x3,4 / 20	Кварцевая стабилизация частоты
19	PK - 1005	1300 (130...175)/ WFM (± 50 кГц)	6			30 • 30 • 20	3 / 48	
20	HKG - 1830	IR (ближний ИК)	25		300 - днем, 700 - ночью	45 • 30 • 18	6 / 20	

Приложение 6. Сводная таблица характеристик устройств несанкционированного съема информации с телефонных линий

Марка	Частота, МГц	Дальность передачи, м	Габариты, мм	Вид модуляции
Телефонные радиозакладки в обычном исполнении				
ЛСТ-5	60-170	200-1000	25х13х10	ЧМ
ЛСТ-7	350-450	300	25х25х7	ЧМ
00-205	140-150	150	60х40х20	УЧМ
РЯО 136	140-144	до 2000	40х24х12	УЧМ
РЯО 139	135-180	до 500	36х12х10	УЧМ
Т1	90-118	до 300	14х13х8	ЧМ
иМ 003	108-112	до 500	22х15х10	ЧМ
иМ 008	136-145	до 700	22х15х10	ЧМ
РТМ-12	64-125	50	36х25х12	ЧМ
РТП-017	130	100	45х15х4	ЧМ
РТП-018	130	-	70х25х4	ЧМ
РТП-020	380-470	-	70х25х4	ЧМ
В закамуфлированном виде под конденсаторы и другие радиотехнические элементы				
НВ-ПТ	130-150	500	3х16х4	ЧМ
НВ-ПТ450	400-500	200-300		ЧМ
РК130	138	150	«рисовое зерно»	ЧМ
РК130-Б	138	800	15х6х11	ЧМ
иМ 008	136-145	до 700	35х15х15	ЧМ
Радиозакладки, установленные в капсулах телефонных трубок				
РК(СШЗАЪ)	-	150	в габаритах камуфляжа	ЧМ
РК155	-	300	048х21	ЧМ
РК1 10-Б	-	250	в габаритах камуфляжа	УЧМ

Окончание приложения 6

Марка	Частота, МГц	Дальность передачи, м	Габариты, мм	Вид модуляции
Комбинированные системы (телефон / микрофонные передатчики)				
ЛСТ-4	100-150	100	35х16х11	ЧМ
ЛСТ-8	350-450	200	25х25х5	ЧМ
БТО-4315	115-150	100	26х22х15	ЧМ
БТО-4317	395-415	100	66х27х14	УЧМ
ПТРМ	88-108	до 250	29х19х12	ЧМ
РК125-SS	139	до 10000 с ретранслятором	-	-
Радиозакладки с индуктивным датчиком				
Ш01т	100-210	до 1000	70х38х20	ЧМ
Ш01ртм	100-210	до 1000	70х38х20	ЧМ
Ш01т	100-210	до 1000	70х38х20	ЧМ
111021т	100-210	до 1000	70х38х20	ЧМ
STG-4320	395-415	250	40х15х15	УЧМ

ЗАКЛЮЧЕНИЕ

В данном пособии дана подробная классификация телекоммуникационных каналов связи и описаны основные технические характеристики и физические свойства каналов. Рассмотрены основные термины, определения и технические характеристики основных технических каналов, по которым проходит утечка информации. В пособии рассматривается физическая природа явлений и процессов, которые лежат в основе утечки информации, такие, как паразитные излучения и наводки, акустоэлектрические преобразования, паразитная генерация, высокочастотное навязывание, причины формирования параметрических каналов утечки информации и т.д.

Приведенная в пособии информация является дополнительной к курсу «Техническая защита информации», носит справочно-технической характер и касается смежных разделов физики, радиотехники, электротехники, теории информации, микроэлектроники и др. дисциплин.

В пособии описаны возможные угрозы безопасности информации при потенциальной возможности ее утечки по техническим каналам, а также приводится характеристики устройств несанкционированного съема информации при реализации информационных угроз. Кроме того, приводится анализ методов и средств обеспечения безопасности информации на объектах информатизации при ее обработке техническими средствами. Детально рассмотрены методы и средства защиты речевой информации.

Авторами большое внимание уделено особенностям технологического обеспечения безопасности на типовом объекте информатизации. Даны рекомендации по организации защиты информации от утечки по техническим каналам на объектах с техническими средствами обработки информации.

Авторы надеются, что данное пособие поможет обучающимся в формировании профессиональных компетенций при изучении и промежуточном контроле курса «Техническая защита информации» у бакалавров направления 10.03.01 «Информационная безопасность» и специалистов специальности 10.05.04 «Информационно-аналитические системы безопасности», а полученная из пособия информация окажется полезной в практической деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Голиков А.М. Сети и системы радиосвязи и средства их информационной защиты: учеб. пособие / А.М. Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 392 с. ISBN 978-5-86889-393-3.

2. Защита информации в телекоммуникационных системах / Г.Ф. Конахович и др. - Москва: СПб. [и др.] : Питер,2017. - 288 с.

3. Калинин, И.А. Основы информационной безопасности при работе в телекоммуникационных сетях: учебное пособие /И.А.Калинин, Н.Н.Самылкина. - М.: БИНОМ. Лаборатория знаний, 2008.

4. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось, 1989. – 365 с.

5. ГОСТ 16465-70 Сигналы радиотехнические измерительные. Термины и определения.

6. ГОСТ 17657-79 Передача данных. Термины и определения.

7. ГОСТ 26599-85 Компоненты волоконно-оптических систем передачи. Термины и определения.

8. Бабурин А.В., Чайкина Е.А., Воробьева Е.И. Физические основы защиты информации от технических средств разведки: Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2006.-193 с.

9. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013.

10. Котоусов А. С. Теоретические основы радиосистем. М.: Радио и связь, 2002. 224 с.

11. Кузнецов В.И. Радиосвязь в условиях радиоэлектронной борьбы. – Воронеж: ВНИИС, 2002. – 145с.

12. Белов, Е.Б. Основы информационной безопасности: учебное пособие для вузов/Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шелупанов. - М.: Горячая линия-Телеком, 2011.

13. Гончаров И.В., Герасименко В.Г., Воробьева Е.И., Дмитриев Ю.В., Технические средства обеспечения информационной безопасности: Методические указания к курсовому проектированию / Под редакцией И.В. Гончарова - Воронеж: Воронежский государственный технический университет, 2005. - 128 с.

14. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

15. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил. ISBN 978-59901488-1-9.

16. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.

17. Технические средства и методы защиты информации: учебное пособие для ВУЗов/А.П.Зайцев, А.А.Шелупанов, Р.В.Мещеряков и др.; под ред. А.П.Зайцева, А.А.Шелупанова. - М: Горячая линия-Телеком, 2012.

18. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие для вузов/П.Б.Хорев. - М.: ФОРУМ, 2015.

19. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2017. - 636 с.

20. Железняк В.К., Макаров Ю.К, Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Спецтехника, 2000. № 4.

21. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации. – М.: ООО «Издательство Машиностроение», 2009.

22. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. - М.: НПЦ «Аналитика», 2010.

23. Железняк В. К. Защита информации от утечки по техническим каналам: учебное пособие / В. К. Железняк; ГУАП. – СПб., 2006. – 188 с.: ил. ISBN 5-8088-0230-X.

24. Хорев А.А. Направленные микрофоны и лазерные акустические системы разведки //Специальная техника. – М.: 2010. – № 4 – С. 2-11.

25. Хорев А.А. Средства акустической разведки: проводные микрофонные системы и электронные стетоскопы//Специальная техника. – М.: 2010. – № 5 – С. 2-15.

26. «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002.

27. Меньшаков Ю.К. Теоретические основы технических разведок.- М.: МГТУ им. Н.Э. Баумана, 2008.

28. Меньшаков Ю.К. Виды и средства иностранных технических разведок. /Под ред. М.П. Сычева. - М.: Изд.- во МГТУ им. Н.Э. Баумана, 2009.

29. Временная методика оценки защищѐнности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счѐт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, Москва, 2002.

30. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. N 282.

31. Хорев А.А. Средства перехвата информации с проводных линий связи//Защита информации. Инсайд. – С. Петербург: 2011. – № 1 – С. 22 –32.

32. «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2002.

33. Хорев А.А. Способы и средства подавления электронных устройств перехвата информации, подключаемых к двухпроводным телефонным линиям//Защита информации. Инсайд. – С. Петербург: 2013. – № 1 – С. 12 – 19.

34. Афанасьев, В.В. Защита информации в сетях сотовой подвижной связи / В.В. Афанасьев. - М.: Радио и связь, 2017. - 538 с.

35. Защита информации в системах мобильной связи. - Москва: СИНТЕГ, 2017. - 176 с.

36. Защита информации в системах мобильной связи: учебное пособие для вузов/под ред. А.В.Заряева, С.В.Скрыля. - 2-е изд.-М.: Горячая линия-Телеком, 2005.

37. Максименко, В.Н. Защита информации в сетях сотовой подвижной связи/В.Н.Максименко, В.В.Афанасьев, Н.В.Волков; под ред. О.Б.Макаревич. - М.: Горячая линия - Телеком, 2007.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. Хорев А.А. Классификация электронных устройств перехвата информации [Электронный ресурс] // URL: https://www.docme.ru/doc/1498092/klassifikaciya-e-lektronnyh-ustrojstv-perehvata-informacii (дата обращения: 13.06.2018).

2. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: http://spymarket.com/ (дата обращения: 13.06.2018).

3. Сайт «Лаборатория ППШ» г. Санкт-Петербург [Электронный ресурс] // URL: http://www.pps.ru/ (дата обращения: 13.06.2018).

4. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: http://www.mascom.ru/ (дата обращения: 13.06.2018).

5. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: https://www.nelk.ru/ (дата обращения: 13.06.2018).

6. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: http://www.sinf.ru/ (дата обращения: 13.06.2018).

7. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: http://www.profinfo.ru/ (дата обращения: 13.06.2018).

8. Сайт компании «Сюртель» г. Москва [Электронный ресурс] // URL: http://www.suritel.ru/ (дата обращения: 13.06.2018).

9. ЗАО ПФ «Элвира» Московская обл. г. Железнодорожный [Электронный ресурс] // URL: http://www.elvira.ru/ (дата обращения: 13.06.2018).

10. Электронный журнал «Системы безопасности связи и телекоммуникаций» – компания «Гротек», Москва [Электронный ресурс] // URL: http://sccs.intelgr.com/ (дата обращения: 13.06.2018).

11. Электронный журнал «Защита информации. Конфидент» – издатель ООО «Конфидент», С.-Петербург [Электронный ресурс] // URL: http://www.confident.ru/ (дата обращения: 13.06.2018).

12. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: http://www.ess.ru/ (дата обращения: 13.06.2018).

13. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: http://asbgroup.ru/izdaniya/zhurnal-bdi/ (дата обращения: 13.06.2018).

ОГЛАВЛЕНИЕ

Учебное издание

ТЕЛЬНЫЙ Андрей Викторович
МОНАХОВ Юрий Михайлович

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 26

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики

Учебное пособие

Издается в авторской редакции

Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Acrobat Reader; дисковод CD-ROM; 3,20 Мб. Загл. с титула экрана.

Тираж 10 экз.

Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых
Изд-во ВлГУ
rio.vlgu@yandex.ru

Институт информационных технологий и радиоэлектроники
кафедра информатики и защиты информации
andre.izi@mail.ru