**Государственное бюджетное профессиональное образовательное учреждение**

**Новосибирский Колледж Почтовой Связи и Сервиса**

**Выпускная квалификационная работа на тему:**

**«Выявление возможностей утечки информации по радиоканалам на основе спектра излучения»**

**Выполнил студент группы ТС-43**

**Насыпов Кирилл Олегович**

**Шабронов А.А.**

**Новосибирск 2021**

**Содержание**

# **Введение**

Знание как правильно получить доступ к защищенной информации – обязательное условие для специалистов в рабочей области информационной безопасности . Для того чтобы охранять информацию нужно знать , как взламывают и получают её злоумышленники . Научиться создавать специальные каналы . И сейчас мы в этом подробно разберемся.

# **1.1. Классификация электромагнитных каналов утечки информации**

Электромагнитные волны имеют важное значение для передачи информации. Их можно передавать как на сотни метров , так и на сотни тысяч километров . Утечка информации по радиоканалу происходит посредством перехвата электромагнитных излучений диапазона , которые передаются от отправителя к адресату. Также можно осуществить взлом сигналов у радиолокационных и радионавигационных сис­тем, радиостанций и систем связи ,систем телеуправления, средств радиотелефонной связи, мониторов ПЭВМ, радиозакладок различного типа, перегово­ров внутри помещений предприятия с помощью беспровод­ных служебных систем связи и пр.

Перехват информации по радиоканалам имеет ряд плюсов по сравнению с другими каналами утечки информа­ции, а именно:

– отсутствует естественный контакт с источником информации;

– на прием сигналов не влияет время года и время суток;

– информация поступает в реальном времени;

– перехват информации осуществляется достаточно незаметно ;

– у источника информации нету сведений о начатом процессе перехвата;

– дальность перехвата ограничивается только некоторыми особенно­стями распространения соответствующего диапазона радио­волн и возможностями источника информации.

Утечка информации по радиоканалу может происходить как без преобразования информационного сигнала, так и с его участием.

В технических средствах генерирования, распростране­ния и приема электромагнитных волн используется большое количество функциональных элементов.

#### **1.2. Перехват сигналов связных радиостанций**

Электромагнитные излучения передатчиков свя­зи, модулированные информационным сигналом, могут пере­хватываться прямым образом с использованием дефолтных тех. средств.

Упрощенная структура типового комплекса средств пере­хвата сигналов связных радиостанций включает:

– *приемные антенны.* Они нужны для изменения электромагнитной волны в электрические сигналы, амп­литуда, частота и фаза которых соотносится аналогичным характеристикам электромагнитной волны;

– *радиоприемник.* Предоставляет поиск и селекцию ра­диосигналов по частоте, усиление и демодуляцию выделенных сигналов, их усиление и обработку;

– *анализаторы технических характеристик сигна­лов.* Определяются параметры сигналов: частотные, времен­ные, энергетические, виды модуляции, структуру кодов и др.;

– *радиопеленгатор.* Позволяет найти направле­ние на источник электромагнитного излучения и его коор­динаты;

– *регистрирующее устройство.* Поставляет запись сигналов для документирования и последующей обработки.

Для перехвата радиосигналов связных радиостанций используют разные виды приемников или радиокомп­лексы.

Так, например, используются приемные устройства AR-3000A, AR-5000, АРК-ЦТ, Winradio 3100i-DSP, радиокомп­лексы OSC-5000, AFK-MK1, АРК-Д1, АРК-ПК-П, R9000-DM-20 (профессиональный радиоприемник – многофункциональ­ный комплекс).

#### **1.3. Перехват радиотелефонных сигналов**

Для перехвата радиосигналов с довольно-таки тяжелой структурой, которая применятся в сотовой или пейджинговой , а также в других видах мо­бильной связи, созданы уникальные принимающие комплексы.

Например, система контроля и использования служебных ра­дио­те­ле­фо­нов сотовой связи стандарта NMT-450 ТТС-1 (фир­ма "Нелк") дает возможность находить и даже позволяет следовать по часто­те исходящие и входящие звонки абонентов мобильной связи, приводить в исполнение отслеживание по частоте за каналом во время разговора по мобильному телефону, вести одновременно авто за­пись разговора на диктофон и т.п. В комплексе используются ПЭВМ и два приемника AR 3000 А.

Для отслеживания текстовых сообщений мобильных телефонов созданы ав­томатизированные станции по перехвату сотовых систем связи. В состав этих станций входят: переносной компьютер, спецдемо­дулятор, принимающее устройство, управляемое компьютером. Нужно просто на экране машины задать номер интересую­щего вас абонента – и комплекс начнет сразу автоматически записывать входящие разговоры , также определять номера звонящих абонентов  к абоненту за которым мы наблюдаем , следить за мобильным объектом при переходе из соты в соту.

Похожие системы есть и для радиотелефонов российской системы "Алтай".

Культивация перехваченного радиосигнала используется с помощью средств тех. анализа. К ним относятся: Stabilock 4051, Stabilock 4032, HP 8920 A/D и др.

Для перехвата типографических передач применяются спе­циальные комплексы типа FAX MANAGER, ФАКС-02, 4600-FAX-INT, и др. Они нужны для того чтобы обеспечить автоматическим перехватом в настоящем времени абсолютно любого числа страниц, которые переда­ются по факс-машине со скоростью от 330 до 9700 бит/с, запись текстового сообщения и служебной информации, вывод их на печать.

Перехват пейджинговых передач происходит с помощью спец. комплек­сов .

Например, разработаны АРК-ПК , АРК-Д1 с использованием программного обеспечения (ПО) СМО-ДЕМ, которое выполняет следующие задачи:

– программное обеспечение , которое настроит приемник на нужные нам частоты, заблаговременно занесённые в файл пейджерных радиостанций;

– прием сообщений, которые передаются в формате PJCSAG со скоростью передачи от 512 до 2400 Бод;

– авто распознавание скорости и полярности передачи;

– регистрация в реестре сообщений, руч­ное декодирование и анализ принятых нами сообщений, мгновенный просмотр полученных сообщений, поиск нужного сообщения по шаблону ;

– запоминание и накопление в базе данных информации об абонентах и ее обновление;

– прием сообщений абсолютно всех абонентов (режим "Обнаруже­ние");

– сохранение содержимого экрана в файле.

####  **1.4. Радиомаяки**

Позволяют осуществлять перехват нужной информации о составе технических средств и местах их установки. Такая информа­ция является очень важной, так как позволяет установить, какие средства обработки и передачи информации устанавливаются в помещениях контролируемой зоны. Кроме того, покупаемая и устанавливаемая техника может обеспечивать заклад­ные устройства, управляемые на расстоянии , то есть дистанционно. Подготовка по организации канала утечки информации содержит в себе и процеду­ру локализации "меченых" тех. средств. Для нужно использовать радиосигнальные маяки.

Радиосигнальные маячки могут устанавливаться , например, в упаковку какого-либо продукта , что позволяет контролировать места размещения закупленных средств вычислительной техники. В системный блок могут встраиваться доп. устройства, которые создаются из стандартных модулей, применяемых в ПК, и прячутся таким образом, чтобы иметь доступ к воспроизводимой или вводимой информации.

Передача на пункт прослушивания , конечно же осуществляется по ра­диоканалу.

#### **1.5. Радиозакладки**

Большой ассортимент видов информационных сигналов заставило создавать и выпускать большое количество различных закладок, обеспечивающих преобразование исходных ин­формационных сигналов в радиоизлучение. Для этих преоб­разований можно использовать различные сочетания ФЭ(физических элементов).

В качестве источников питания закладных устройств также можно использовать электрические цепи:

– теле­фонной линии за счет гальванического подключения или ис­пользования специальных сетевых блоков питания;

– силовой, осветительной сети;

– термоэлектрических генераторов;

– детекто­ров СВЧ-энергии.

Также закладное устройство может использовать свой источник питания : радиоизатопную батарею и другие химические источники.

Выбор источника питания обусловливается местом , куда мы будет ставить наш радиомаячок . Наиболее популярны радиозакладки по типу , радиомикрофонов ( чтобы прослушивать перехваченную информацию ) .

***Радиомикрофоны.*** Радиомикрофоны хороши тем , что у них довольно таки простая конфигурация , плюс дешевые комплектующие для их создания , ну и конечно крохотные размеры .Радиомикрофоны существуют непрерывного действия ,управляемые дистанционно , а также с системой VOX (то есть когда появляется речевой сигнал , микрофон включается и начинает записывать).

Микрофоны состоят из: модуля передатчика , выносной антенны , блока питания и микрофона.

Благодаря своей чувствительности, такие микрофоны спокойно могут обхватывать зону в 20 м2.При маскировки такого микрофона, делают отверстие от 3 до 5 мм. В основном почти все такие радиомикрофоны работает в диапазоне от 300 до 500 мГц. В таком диапазоне легче удается достичь приемлемых характеристик для прохождения радиосигнала. Выходная мощность передатчика находится из условий использования и требуемой дальности. Чаще всего в радиомикрофонах используются гибкие внешние антенны , выглядят как отрезок многожильного провода , длинною в четверть волны .

Сетевые блоки дают возможность использовать радиомикрофоны неограниченное время , т.к. питание подается от телефонных или других электрических сетей .

Места где обычно устанавливают радиомикрофоны:

– электрические розетки и выключатели;

– телефонный аппарат;

– горшочки и вазы для цветов;

– письменные приборы;

– мебель (столы, стулья, шкафы, зеркала);

– бытовые приборы (чайники, телевизоры, обогревате­ли, приемники, таймеры);

– элементы конструкции здания (вентиляционные сис­темы, батареи отопления);

– системы электрических соединений (распределитель­ные устройства, коробки);

– предметы интерьера (картины, шторы).

Частенько такие микрофоны маскирую, чтобы было еще тяжелее найти, а маскируют под все что угодно , например : под предметы быта или же оргтехнику.

Рассмотрим некоторые типы таких микрофонов.

**РМК061*.***Данная конструкция выглядит как ,

прямоугольная платка 23х9х6 мм, залитая герметиком со встроенным микрофоном , удобную гибкую антенну и выходы для подключения к питанию от 3 до 6 В.

Этот радиомикрофон является чуть ли не классикой у злоумышленников , поскольку он универсален , также он содержит кварцевый стабилизатор . Прием сигналов от радиоприемника можно осуществить с помощью спец. приемников или сканеров с частотной широкополосной модуляцией частоnы , этот режим называется WFM .

**РМК191.** Этот радиомикрофон создан для того чтобы скрытно размещать его на одежде , например под галстуком .Не обязательно выносить его на улицу , т.к. зона прямой видимости составляет целых 100 метров , а работает без прямого питания около 3 часов .

Существуют и по серьёзней микрофоны например: РК-260 ( без прямого питания работает около 750 часов ) , РК-270 ( только вдумайтесь он работает без питания целый год !) , есть микрофон РК 575 он выглядит как обычная зажигалка , или же РК 585 он выглядит как простая шариковая ручка , а есть в виде гвоздя это РК 520 ; и таких микрофонов огромное количество . Такие радиомикрофоны становятся все совершеннее и все менее заметнее, также стараются повысить зону для дистанционного управления.

***Другие типы радиозакладок.*** Также для взлома электронных сигналов устанавливают специальные закладки в накопители информации ( которые работают на магнитных дисках ), также могут установить в клавиатуру (для вывода информации , например какого-нибудь пароля) и в самом системный блок . Такие закладки очень противные , во-первых их трудно найти , во-вторых они могут месяцами питаться от источников напряжение вычислительной технике и могут передавать информацию на 2 км .

Для съема электрических сигналов созданы специальные закладки , по типу SIPE 005, НВ-ПТ ( выгладит как конденсатор ).

 Для съема акустической информации по виброакустиче­скому каналу созданы хитрые и уникальные радиостетоскопы: STG 4025 (пе­редатчик-стетоскоп, дальность 250 м, масса 18 г) STG 4027(передатчик-стетоскоп, дальность 200 м, масса 25 г) , AD-50 (радиостетоскоп, дальность 100 м, масса 120 г), РК 1005 (пере­датчик-стетоскоп, дальность 500 м, масса 13 г).

Для того чтобы снять видеосигнал созданы специальные видеокамеры с передачей изображения по радиоканалу . А для снятия оптических сигналов с волоконных линий связи , созданы закладки с перехватом нужной информации с помощью светодиодов.

**Расчетная часть**

За основу брал сканер RTL2832 . Стоимость 20 долларов .

Технические характеристики:

1) Диапазон частот составляет от 100кГЦ – 1750 МГц.

2) Модулирует – AM, FM, NFM, LSB, USB, CW.

 AM – амплитудная модуляция ;

 FM , NFM – частотная модуляция и узкополосная частотная модуляция ;

 LSB – нижняя амплитудная модуляция ;

 USB – верхняя амплитудная модуляция ;

 CW – непрерывная однополосная модуляция.

3) Полоса обзора меняется от 250 кГЦ до 3МГц

4) Чувствительность составляет 0.22 мКв (на 438 МГц в режиме NFM)

5) Входное сопротивление приемника – 50 Ом

Имеются 2 разъема SMA на материнской плате . Первый это UV от 24-1750 Мгц , а второй HF 100 кГц – 24 МГц . В центре самой материнской платы находится TV-тюнер.

Плата нашего TV-тюнера на микросхеме RTL2832 + R802T .В общем при подсоединению к ПК очень важно сначала подсоединить антенну R802T к нашему тюнером , а же потом вставлять сам тюнер в наш ПК , через USB-порт . Вызвана такая предосторожность тем , что разряд статического электричества может повредить наш ПК.

Принцип работы заключается в следующем : От антенны мы подсоединяемся R802T . Дальше сигнал преобразуется , понижается частота , происходит фильтрация , после чего сигнал подается на микросхему RTL2832 , которая является мозгом всего приемника и уже в ней сигнал оцифровывается и уже после данные отправляются через шину USB в компьютер , но это если говорить простыми словами . Если говорить подробно , то происходит следующее : Сигнал с антенны подается через полосовой фильтр , который подавляет частоты не входящие в полосу приемника .

На входе в микросхему стоит усилитель , после которого снова стоит фильтр уже перенастраиваемый , затем сигнал подается на смеситель в который также подается частота с внутреннего генератора тактирующегося от кварцевого резонатора , потом сигнал отфильтровывается еще одним перестраиваемым фильтром и снова усиливается , в результате на выходе микросхемы частота сигнала понижается для возможности оцифровки . В общем сигнал подается на RTL2832 . Сигнал с пониженной частотой подается на АЦП , после чего в цифровом виде получают квадратуру сигнала для дополнительной обработки и фильтрации , затем происходит передискритизация , то есть изменение частоты дискретизации в более удобный вид для обработки внутри микросхемы . Микросхема анализирует и подстраивает различные элементы схемы оцифрованный сигнал децимируется , то есть частота дискретизации понижается до 3 MSPS (мега сэмпл в секунду ) и меньше , после передается через USB в компьютер . Микросхема R820T и микросхема RTL2832 тактируются от одного и того же кварцевого резонатора с частотой 28.8 МГц. А общение между нашими микросхемами происходит через шину I2C.

Также не стоит забывать , чтобы воспользоваться нашим тюнером , нам нужно установить на него драйвера . Для начала скачивает программу SDRsharp , именно с помощью него можно просматривать радиоэфиры .

Ну а вообще нужно ответить на вопрос “А что вообще можно послушать с SDR “?

Возможности у приемника RTL2832 такие :

-Послушать радио своего города от 88-115 МГц ;

-Переговоры самолетов и диспетчеров от 120-134 МГц ;

-Портативные радиостанции 430-460 МГц ;

-Вещание телевидения 470-860 МГц ;

-Каналы какого-нибудь такси там диапазон около 862 МГц ;

-Также можно найти радиолюбителей они примерно от 140-150 МГц.

Причем чтобы прослушивать цифровое телевидение , нам понадобится программа DSD , она  позволяет цифровую передачу на устройстве записи по умолчанию, и проигрывает декодированный результат в устройство воспроизведения по умолчанию . Чтобы соединить SDR и DSD нужен будет Virtual Audio Cable .

Вообще понадобится следующий список программ для комфортной работе на SDR и как правильно их установить:

1)Нужна последняя версия SDR# Dev и SDR# RTLSDR Plugin , а также  библиотеку RTLSDR

2) Распаковываем в один каталог SDR# Dev и SDR# RTLSDR Plugin. Из библиотеки RTLSDR в этот же каталог кладём файл rtlsdr.dll (он в архиве в каталоге x32). Из подкаталога config файл SDRSharp.exe.config выносим на уровень выше (туда где основная масса файлов получилась).

3) Также нужно скачать программу Zadig - программа для замены драйвера тюнера . Т.к. если просто вставить наш тюнер в ПК , то ПК посчитает , что это флешка и поставить соответствующие ошибочный драйвера .

4) Запускаем Zadig.exe, тыкаем пункт Options->List all devices, далее выбираем Builk-in, Interface 0, выбираем драйвер для замены — «WinUSB», жмём Reinstall Driver, со всем соглашаемся.

5) После чего запускаем SDRSharp.exe, в левой части меню — будет неактивная кнопка Frontend, и напротив неё — выпадающее еще одно меню. Выбираем там RTL-SDR / USB, и жмем Play в левом верхнем углу.

6) После в программе можно будет вбивать нужные нам частоты или же использовать ползунок по всему радиоканалу , методом перетаскивания .

Также не стоит забывать что существует WebSDR , это тот же самый SDR , только находится в браузере . Объясню по - подробней что это такое .

WebSDR это программный радиоприемник, подключенный к сети интернета, который позволяет огромному количеству радиолюбителей принимать и настраивать его когда угодно зайдя на web-сайт через интернет.

96,5% всех WEBSDR приёмников работают на КВ или же транслируют местный канал УКВ. Но есть и такие приёмники, которые смотрят в верх в небо ,и слушают космос на радиолюбительских частотах работы земных спутников. Основные из них:  R4UAB SAT WEBSDR, Microwave WebSDR in Farnham, WebSDR in Central NJ-USA и WebSDR on ZR6AIC in Johannesburg . И каким способом они помогают в научных целях ? Ответ очевиден – принимать через них телеметрию с космического аппарата .

Но мы отвлеклись . В целом это удобно . Не нужно покупать тюнер который стоит 600 или же 1200 рублей , вообще ничего не нужно покупать , главное прост зайти на сайт , выбрать нужный нам эфир и сидеть на нем , несомненно это плюс . Без вложения попасть на радиоканал и прогуливаться по нему очень интересно . Однако есть и свой минус . Ограниченность частоты каналов . Допустим у нас есть физический купленный приемник такой как RTL2832 у него радиус от 100 КГц до 1700 МГц . Зайдем же на сайт WebSDR и выберем любой из списка . Первый попавшийся JO32KF от 0 до 29 Мгц , второй IO70JB – частота от 104 Мгц до 105 МГц , GG56TV – у него даже несколько диапазонов 0.000 - 2.048 MHz, 1.804 - 1.996 MHz, 3.494 - 4.006 MHz, 6.894 - 7.406 MHz, 13.994 - 14.506 MHz , 26.966 - 29.014 MHz , 143.963 - 146.011 MHz , 145.976 - 148.024 MHz . Казалось бы у него много диапазонов , но вот у них скажем так маленькие “границы “ . Что по вашему лучше ? иметь один единственный диапазон 100Кгц-1700Мгц или же маленькие раздроблённые кусочки ? И поэтому я и выбрал физический приемник . Так в разы удобней . Но для ознакомления конечно же лучше для начала опробовать именно версию SDR’а “web” , чтобы узнать как это работает.

Также можно сравнить физические sdr приемники и объясню почему именно выбрал RTL2832 .

Возьмем к примеру TZT B210 он работает в диапазоне от 70 МГц до 6 ГГц. Вопрос думаю сразу отпадает если узнать , что такое удовольствие стоит аж 75000 тыс. рублей . У него хороший диапазон и даже хорошие отзывы среди обеспеченных радиолюбителей . Но в обычных целях просто побегать по каналам и поискать радиолюбителей или же поискать радиостанции вполне хватает дешевого китайского RTL2832 . Или же возьмем чуть дешевле приемник . Baofeng DM-4R . Стоимость у него 4500 рублей . Рабочий диапазон 136-174 мгц , 400-800 мгц. Виды модуляции он поддерживает только DM и FM . Однако это устройство можно таскать с собой поскольку это рация . Ну во-первых статичный наш RTL2832 подерживает гораздо больше видов модуляции , если b210 поддерживает только DM и FM , то RTL2832 поддерживает AM, FM, NFM, LSB, USB, CW. Да нету дельта-модуляции , но для радиоканала нам по факту нужна только FM модуляция , соответсвенно зачем мне FM приемник за 4500 рублей , если есть приемник за 1500 реблей ? Тем более , тут уже подходит второй пункт . И наконец во-вторых , у RLT диапазон от 100 КГц до 1700 МГц , а у B210 136-174 мгц , 400-800 мгц. Конечно стандартная антенна очень плохая у RLT2832 , что идет с ним в комплекте , когда стандартная выигрывает у B210 , но ведь при возможности можно докупить телевизионную антенну для нашего RLT2832 . Допустим антенна Selenga 100 . У нее рабочий стандарт такой же как и у baofeng b 210 UHF/VHF . У UHF - 87.5-230 МГц , у VHF - 470-862 МГц . Явно видно преимущество в плане характеристик у RTL 2832 с антенной Selenga 100 . Поэтому в сумме затраты уйдут на 1630 рублей , а не 4500 .

**Методы защиты радиоканалов**

Также в этом разделе хочу описать какие существуют методы защиты радиоканалов . В настоящее время существует 2 популярных вида для защиты радиоканала . Первый – криптографический , второй – шумоподобные сигналы . Начнем с первого метода – криптография .

Криптография – это наука об обеспечении конфиденциальности информации.

Сами методы криптографического преобразования делятся на 4 вида :

1. Шифрование
2. Стенография
3. Кодирование
4. Сжатие

Для шифрования информации используется ключ , а также сам алгоритм преобразования . Алгоритм , как правило является неизменным для почти любого вида шифрования . Сам ключ содержит в себе информацию для управления , которая в свое время определяет выбор преобразования на определенных шагах алгоритма величины операндов , которые используются при реализации алгоритма шифрования . Операнд – объект надо которым проводятся операции.

Методы стенографии позволяют скрыть как смысл хранящийся или передаваемой информации , так и факт передачи или хранения информации. В основе всех методов стенографии находится маскировка закрытой информации среди открытых файлов , то есть маскируется секретные данные и при этом параллельно создаются реалистичные данные , которые по просту нереально отличить от настоящих . Скрытый файл тоже может быть зашифрован . Если кто-нибудь случайно наткнется на этот файл , то зашифрованная информация будет воспринята как ошибка или сбой в системе .

Кодирование – основной задачей является замена наших слов , предложений на коды . Как правило коды используют сочетания букв , знаков , цифр . Как при кодировании , так и при обратном преобразовании используются спец . словари или же таблицы . Также не стоит путать кодирование и шифрование абсолютно разные вещи . Например для восстановления закодированного сообщения , нужно просто знать простое правило замены , когда для расшифровки нужен еще и ключ к шифру .

Сжатие информации тоже является своего рода криптографией , но с определенной оговоркой . Цель сжатия – сокращение объема информации . Но и в тоже время сжатую информацию нельзя просто так взять и прочитать , нужно все тоже обратное преобразование . Но сжатие в наше время доступно каждому человеку . Сжимать информацию можно через WINrar или же 7Zip . Соответственно сжатие в наше время является наименее полезным криптографическим методом в качестве защиты информации .

Метод шифрования – это совокупность преобразований свободной информации в закрытую . Большинство шифров уже устарело , но есть редкие исключения .

В настоящее время есть несколько популярных методов шифрования , такие как : 3DES , Data Encryption Standard , International Data Encryption Algorithm .

Эти алгоритмы сообщения шифруют блоками по 64 бит. Если объем сообщения превышает 64 бита , то необходимо разбить блоки по 64 бит , а затем свести их воедино , при помощи 4 основных методов :

1. электронной кодовой книги (Electronic Code Book, ECB);
2. x-битовой зашифрованной обратной связи (Cipher FeedBack, CFB-x);
3. цепочки зашифрованных блоков (Cipher Block Changing, CBC);
4. выходной обратной связи (Output FeedBack, OFB).

3DES – это блочный шифр по типу DES , который был создан для устранения неполадка в виде короткого ключа DES (56 бит) , который могли взломать методом перебора . Скорость Triple DES в 3 раза меньше чем у DES , однако криптостойкость выше на голову .

AES – этот стандарт шифрует блоки по 128 бит , 192 , 256 .

Также есть методы для преобразования исходного речевого сигнала , где голос будет не узнаваем , а слова не понятны и не разборчивы . Такой метод называется - аналоговое скремблирование . Что удивительно этот сигнал , который маскируют , находится в том же спектре , как и исходный сигнал . Необходимым свойством такого преобразования является возможность обратного преобразования для восстановления речевого сигнала на приемной стороне. Тех. средства , что обеспечивают защиту информации методом аналога – называются скремблерами . Также они еще известны как – маскираторы речи . Но не смотря , на их эффективность все же в сигнале закрытого скремблера сохраняются отдельные частицы речевого сообщения .

Если оценивать в целом , то аналоговые методы защиты информации для речевого сигнала по сравнению с цифровыми проигрывают в качестве и даже эффективности . Однако эти методы дешевы , просты , а также характеризуются высоким качеством восстановленного речевого сигнала .

При методе скремблирования преобразования сигнала возможно по 3 параметрам : частоте , амплитуде , времени . Но в системах подвижной радиосвязи практическое применение нашли в основном временные и частотные преобразования сигнала , а также их комбинации . Из-за возможных помех в радиоканале существенно затрудняются точные восстановления амплитуд речевого сообщения , поэтому амплитудные преобразования при скремблировании по факту не применяются .

При частотных преобразований сигнала в средствах подвижной радиосвязи используются следующие виды скремблирования :

1. Разбиение полосы частот речевого сообщения на несколько поддиапазонов и частотная инверсия спектра в каждом относительном средней частоты поддиапазона .
2. Частотная инверсия .
3. Разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки .

При временных преобразований преобразуется разбитие сигнала на речевые сегменты сообщения и их перестановки по временному параметру . Используются за частую 2 популярных вида :

1. Временные перестановки сегмента речевого сообщения .
2. Инверсия по времени сегментов речи .

Комбинированные методы преобразования сигнала предполагают , что использование сразу нескольких тех . способов скремблирования повысит эффективность , но они ограничиваются возможностями тех. реализацией аналоговых скремблирований .

Также у скремблирования существуют свои основные характеристики .

Первая характеристика – уровень закрытой информации . Стоит отметить , что , если речь идет о сложных цифровых систем передачи информации , понятие уровня закрытой информации строго обсуждается и определяется криптографической стойкостью информации , когда у аналоговых скремблеров данной понятие носит условный характер , потому что в настоящее время у них нет четких стандартов или правил . В ряде случаев в качестве особенных критериев уровня закрытой информации при обзоре и сравнения разных средств защиты подвижной радиосвязи с аналоговым скремблированием , вполне можно использовать кол-во ключевых параметров и кол-во возможных ключей скремблера .

Под ключевым параметром аналогового скремблера обычно понимается какой-либо параметр изменения речевого сообщения , значение которого нужно знать для реализации обратного преобразования сигнала на принимающей стороне .

Ключом аналогового скремблера , понимается конкретное секретное состояние некоторых параметров преобразования речевого сообщения . Количеством ключей скремблера назначается множеством всеизвестных значений ключа . Для скремблера с одним ключевым параметром оно определяется принципам числа возможных состояний этой функции , для скремблера с несколькими ключевыми функциями – кол-вом возможных вариантов комбинаций значения этой функции .

Качество восстановления сигнала – это искажение сигнала при его частотном или временном преобразовании . Это хар-ка показывает понятность и узнаваемость текста . Наилучшим качеством восстановления сигнала являются частотные инверторы , которые в принципе не ухудшают понятность и узнаваемость речи при правильном использовании .

Более тяжелые способы частотных преобразований имеют право вносить некоторые искажения в речевое сообщение . Исполнение высокого качества восстановления речевого сигнала при временном преобразовании требуют весьма тяжелой обработки .

**Раздел практическое применение**

После того как я объяснил почему выбрал свой приемник ,написал тех.параметры и описал какие у него возможности , мы плавно переходим к практическому применению . В данном разделе я подробно опишу , что мне удалось найти на радиоканалах .

Ну во-первых захожу в программу SDRsharp и там выбираю пункт RTL-SDR (USB). Затем поднимаем усиление нашего приемника в настройках до 37,2 дБм.

Дальше начинаю ходить по радиоканалу .

Первый интересный канал связи который я нашел был на частоте 171.269 Мгц. Здесь я отчетливо услышал как люди переговаривались по рации на обычные будничные темы . Несложно догадаться , что это обычные радиолюбители .