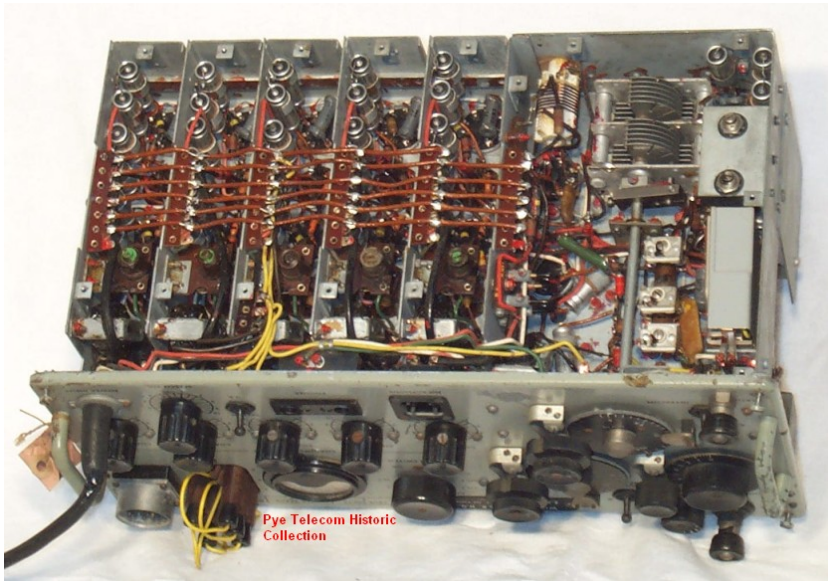
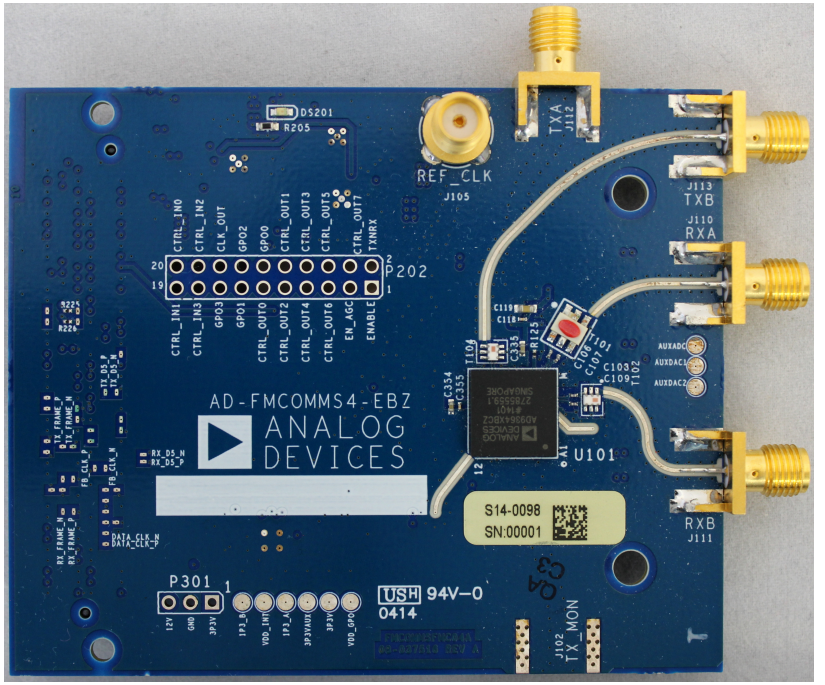
SDR — радиоотмычка XXI века

Радиосвязь: от аналога к цифре





SDR: Hardware

RTL2832U based TV-stick

+

- Малые размеры
- Достаточно широкий диапазон (60 — 1700 МГц)
- Обзорная полоса 3,2 МГц
- Дешевизна

-

- Высокая шумность
- Слабая чувствительность
- Работа только на прием

SDR: Hardware

HackRF One

\+

- Малые размеры
- Широкий диапазон
(10 — 6000 МГц)
- Полоса пропускания в 10 МГц
- Относительная дешевизна

\-

- Слабая чувствительность
- Прием и передача только
в режиме полудуплекса.

SDR: Hardware

bladeRF

+

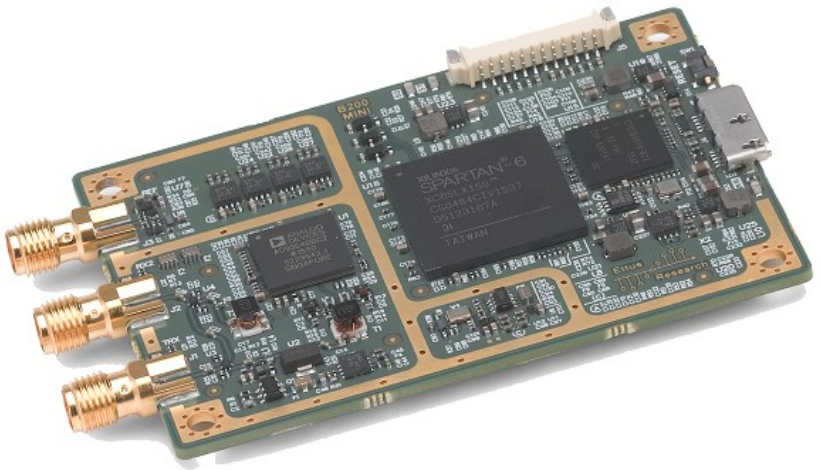
- Малые размеры
- Полоса пропускания в 28 МГц
- Полный дуплекс
- Высокая чувствительность

-

- UHV-SHF диапазон 300Mhz — 3.8 GHz
- Относительно высокая цена

SDR: Hardware

Ettus Research USRP



+

- Разнообразные варианты сменных плат расширения
- Полоса пропускания в 56 МГц
- Полный дуплекс
- Отличная поддержка

-

- Цена

SDR: Software

GnuRadio упрощает процесс создания DSP схем, представляя их в виде графа, элементы которого являются отдельными блоками выполняющими требуемую функцию.

SDR: Software

- Позволяет создавать программные радиоприемники и радиопередатчики
- Позволяет создавать схемы обработки сигналов в графическом режиме
- Со схемой обработки сигналов можно связать графический интерфейс, и управлять параметрами интерактивно
- В наличии богатая база готовых блоков для цифровой обработки сигналов
- Можно писать свой софт для ЦОС, используя библиотеки GnuRadio
- В качестве источников сигнала можно разнообразное оборудование
- Благодаря открытым исходникам имеется возможность безгранично расширять функционал
- Процесс ЦОС при помощи GnuRadio очень нагляден, что позволяет использовать его в учебном процессе

Проблемы безопасности радиоустройств

- Подверженность replay атакам
- Уязвимая криптография
- Большое количество legacy оборудования
- Использование в критических системах источников данных уязвимых к подмене

Шалости с HackRF One: replay attack

При помощи идущей в комплекте с HackRF утилиты, мы можем записать, а затем транслировать заново копию всего того что передавалось в эфире.

Данная утилита великолепно подходит для проведения replay атаки.

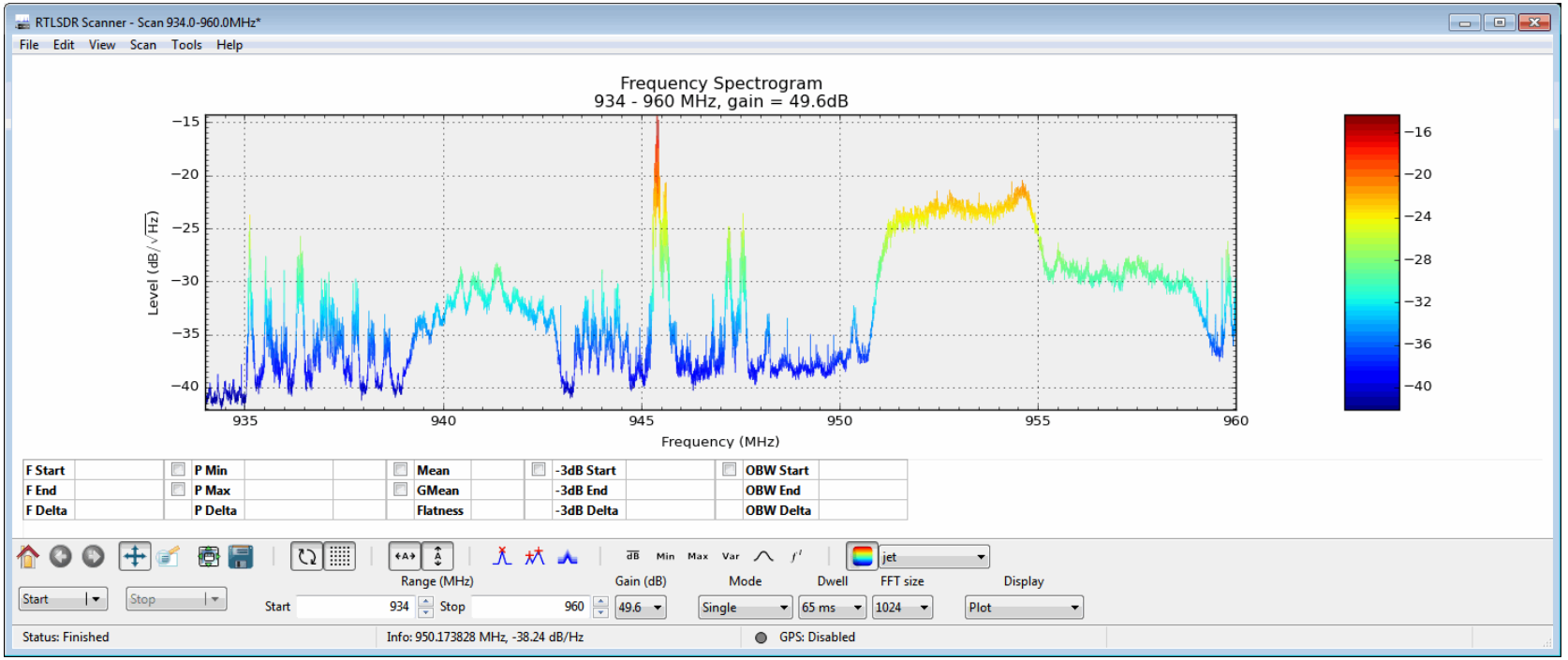
Replay attack

Множество устройств с радиоуправлением основаны на приемниках с фиксированным кодом. И эта розетка — из их числа.

Пеленгация

http://rtl-sdr.sceners.org/?p=385

RTLSDR Scanner



Телефон DECT: Ваш разговор кое-как защищен. Иногда.

Слой управления доступом к данным DECT также предоставляет шифрование в соответствии со стандартным криптографическим алгоритмом DECT — DECT Standard Cipher (DSC). Шифрование является довольно слабым: используется 35-разрядный вектор инициализации, аудиопоток защищается 64-битным шифрованием.
© Wikipedia

«предоставляет»?

GPS: Global Position for Susanin

В настоящее время систему GPS широко используют в разных областях, и доверяют ей

ЗРЯ!

Стоимость оборудования для подмены GPS сигнала равна стоимости HackRF