|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| logoМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума) | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнил студент Костенецкий И.В.  гр. С8117-10.05.01ммзи | | | | | | | | |
|  |  |  | | | | | |  | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Старший преподаватель кафедры информационной безопасности ШЕН | | | | | | | | |
|  | | | |  | С.С. Зотов | | | | |  |  |  | | | | |  | С.С. Зотов | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « | 16 | » | января | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « | 16 | » | января | | | | | | 2021 г. |  |  | с | « | 22 | » | февраля | | | | 2021 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июня | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Кафедра информационной | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ШЕН ДВФУ | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 | | | | | | | | | | | | | | | | | | | | |

# Характеристика

Выдана студенту 4 курса, специальности «Компьютерная безопасность», специализация «Математические методы защиты информации», Костенецкому Илье Владимировичу.

Костенецкий Илья Владимирович, в период с 22.02.2021 по 26.06.2021 года, проходил учебную практику (учебно-лабораторный практикум) на кафедре информационной безопасности ШЕН ДВФУ.

За время прохождения практики Илья проявил усердие, тягу к знаниям, огромное желание и трудолюбие, а также неподдельный интерес к изучению материала. Приходил на консультацию вовремя с перечнем вопросов, с подробным и исчерпывающим описанием о текущем состоянии практики, со списком отмеченных задач. Внимательно изучал предложенные материалы и литературу на интересующую тематику.

Костенецкий И.В. полностью выполнил предусмотренную программу практики, продемонстрировал умения самостоятельно решать практические вопросы, применяя теоретическую базу, полученную в учебный период, а также при самостоятельном обучении.

При выполнении поставленных задач Костенецкий И.В. характеризуется инициативностью, сообразительностью и ответственностью.

Старший преподаватель кафедры

информационной безопасности ШЕН \_\_\_\_\_\_\_\_\_ Зотов С.С.

# Дневник практики

|  |  |  |  |
| --- | --- | --- | --- |
| Дата | Рабочее место | Краткое содержание выполняемых работ | Отметки руководителя |
| 22.02.21 – 22.03.21 | КИБ | Ознакомление с устройством «HackRF» |  |
| 23.03.21 – 27.04.21 | КИБ | Работа с программным обеспечением «SDRsharp» |  |
| 28.04.21 – 1.06.21 | КИБ | Разработка проекта в «GNU Radio» |  |
| 2.06.21 – 14.06.21 | КИБ | Написание предварительного отчёта по проделанной работе |  |
| 15.06.21 – 20.06.21 | КИБ | Внесение правок в отчет |  |
| 21.06.21 – 26.06.21 | КИБ | Сдача готового отчета преподавателю |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Костенецкий И.В.\_\_\_\_\_\_\_

подпись Ф.И.О.

Руководитель практики от ДВФУ \_\_\_\_\_\_\_\_\_\_\_\_\_\_Зотов С.С. \_\_\_\_\_\_\_

подпись Ф.И.О.

**Оглавление**

[Характеристика 2](#_Toc75196496)

[Дневник практики 3](#_Toc75196497)

[Задание на практику 5](#_Toc75196498)

[Введение 6](#_Toc75196499)

[1 Описание устройства HackRF 7](#_Toc75196500)

[2 SDRsharp 11](#_Toc75196501)

[3 Анализатор спектра в Gnu Radio 14](#_Toc75196502)

[Заключение 16](#_Toc75196503)

[Список использованных источников 17](#_Toc75196504)

# Задание на практику

* Ознакомление с устройством «HackRF».
* Ознакомление с принципами работы с программным обеспечением для «HackRF».
* Написание отчета по проделанной работе.

# Введение

Учебная практика (учебно-лабораторный практикум) проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 22 февраля 2021 года по 26 июня 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков написания научных статей, с целью подготовки к написанию дипломной работы.

Задачи практики:

1. Теоретически изучить принципы работы с программой «SDRSharp».
2. Разработка анализатора спектра с помощью программного инструментария «GNU Radio».
3. На основе полученных знаний написать отчет по проделанной работе.
4. Разобраться в данной теме, уметь определять вопросные моменты в этой сфере.

# 1 Описание устройства HackRF

Для начала разберемся, что такое SDR. Согласно Википедии, программно определяемая радиосистема (англ. Software-defined radio, SDR) — радиопередатчик и/или радиоприёмник, использующий технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, за исключением изменения рабочих параметров, используемых в ходе обычной предварительно определённой работы с предварительными установками радиоустройства, согласно той или иной спецификации или системы.

ПОР выполняет значительную часть цифровой обработки сигналов на обычном персональном компьютере или на ПЛИС. Целью такой схемы является радиоприёмник или радиопередатчик произвольных радиосистем, изменяемый путём программной переконфигурации (отсюда происходит альтернативное наименование таких систем - программно конфигурируемые).

HackRF One — это дешёвая, с открытым исходным кодом платформа Software Defined Radio.

HackRF One имеет следующие характеристики:

1. Диапазон частот: 1 MHz – 6 GHz;
2. Полоса пропускания: 20 MHz;
3. RX ADC bits (биты на вход): 8;
4. TX DAC bits (биты на выход): 8;
5. TX кабель: да;
6. Гнездо антенны: SMA female;
7. Дискретизация: 8–20 Msps;
8. Панадаптеры / Приемники: 0/1;
9. Полудуплексный ресивер;
10. Увеличение модности приёма и передачи, а также фильтр частот настраивается программно;
11. Программно-констролируемая мощность порта антенны: (50 mA на 3.3 V);
12. Штырьевой разъём для подключения дополнительных плат, увеличивающих функциональность;
13. Интерфейс хоста: USB 2.0;
14. Поддерживаемые операционные системы: Windows, Linux, Mac.

Как можно увидеть, у устройства довольно медленный интерфейс USB 2.0, а также частота пропускания только 20 MHz, то есть это не самый «ТОП». Но для обучения этого хватит. К тому же, за последнее время на устройство сильно снизилась цена. И ещё, хотя в характеристиках указана поддерживаемая частота 1 MHz – 6 GHz, но можно выйти за этот диапазон чуть ниже и чуть выше.

У этого устройства прошивка с открытым исходным кодом. Оно совместимо с GNU Radio, SDR# и другими программами. Хорошая совместимость с Linux.

Нельзя запускать приём или передачу данных без подключённой антенны! Это очень важно, поскольку прибор не контролирует, подсоединена ли антенна и в любом случае под нагрузкой подаёт электричество, поэтому без антенны HackRF может просто сгореть.

При подключении к компьютеру HackRF на нём загораются индикаторы.

Первые три индикатора:

1. 3V3
2. 1V8
3. RF

Это индикаторы питания различных элементов. Они могут гаснуть при включении режима экономии энергии. 1V8 и RF могут гаснуть, если HackRF ничего не делает. Но при работе HackRF (приём и передача данных) все три должны гореть. Если какой-либо из них не горит, то это означает, что имеется проблема.

Следующий: USB

Когда он горит, то это означает, что компьютер «общается» с HackRF как с USB устройством. Этот индикатор загорается чуть позднее первых трёх.

Последние два:

1. RX — означает операции приёма данных
2. TX — означает операции передачи данных

Последние три индикатора находятся под управлением программного обеспечения. Поэтому можно установить пользовательскую прошивку и переназначить их функции.

Что касается цветов, то они вообще ничего не означают: цвета разные только чтобы вы могли отличать светодиоды друг от друга.

Теперь рассмотрим кнопки.

RESET — сбрасывает, перезагружает микроконтроллер. Аналог отключения и подключения USB шнура.

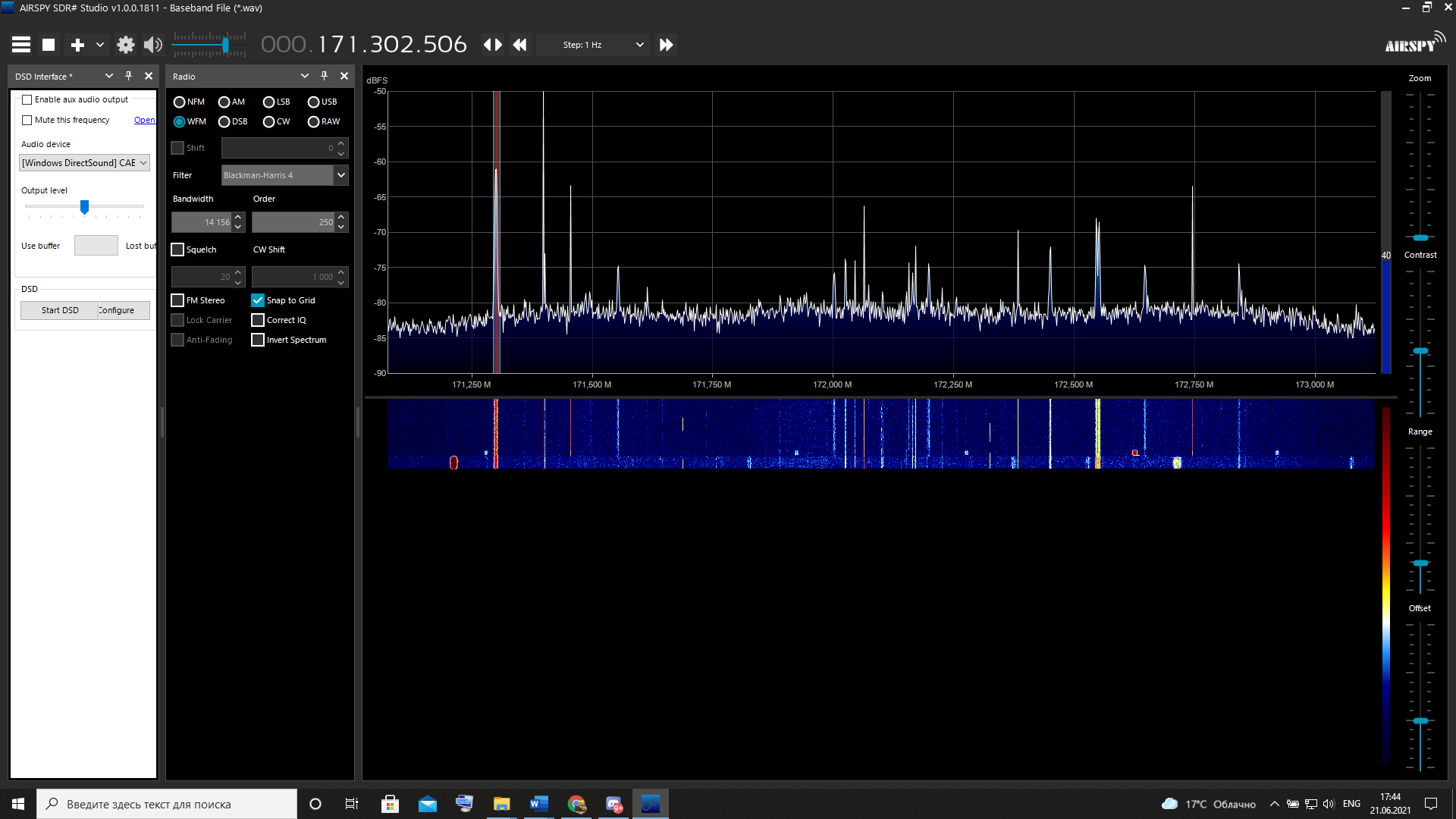
DFU — режим обновления прошивки. На самом деле при обновлении прошивки этот режим не нужен. HackRF может обновлять свою прошивку без перехода в этот режим. Главная функция этой кнопки — это раскирпичивание устройства.

Эта кнопка функционально только при включении устройства или нажатии кнопки RESET. Всё остальное время эта кнопка не выполняет никаких функций, поэтому при установлении пользовательской прошивки этой кнопке можно назначить какую-нибудь функцию ввода.

# 2 SDRsharp

SDRSharp — одна из популярных и простых в использовании программ под Windows для работы с RTL2832 (и некоторыми другими SDR). При старте нужно выбрать RTL2832, нажав на кнопку Front-end. Вводить частоту руками нужно в поле Center.

Слева вверху — выбор типа демодулирования. FM используется для обычного FM-вещания и аудио в аналоговом телевидении, AM — в радиостанциях на низких частотах и переговоров самолетов, NFM — в рации.



Многие внешние декодеры цифровых передач работают через «аналоговый» интерфейс — то есть ты запускаешь SDRSharp, устанавливаешь программу Virtual Audio Cable (программа платная), настраиваешь SDRSharp, чтобы он декодированный звук выводил в VAC, и в системных настройках Windows указываешь VAC как устройство записи по умолчанию. В результате внешняя программа-декодер будет получать звук от SDRSharp.

Таким образом подключаются декодеры P25 раций (милиция), данных с метеоспутников, пейджеров, навигационных сообщений самолетов (ADS-B) и многого другого. Такой необычный способ подключения сложился исторически — раньше к компьютеру подключали аналоговые приемники. Со временем декодеры дописывают, чтобы они напрямую работали с RTL-SDR.

Что послушать в радиоэфире?

Радиопереговоры в безлицензионных диапазонах

Гражданские рации, не требующие регистрации в России, работают на частотах 433 и 446 МГц. Впрочем, в Москве русскую речь там услышать сложно. Их сразу и без проблем слышно в SDRSharp, модуляция NFM.

Поскольку каналов много, очень полезен плагин для SDRSharp AutoTuner Plugin — он автоматически включает частоту, на которой ведется передача, и таким образом можно слушать сразу все каналы раций.

Радиопереговоры полиции

Полиция во многих регионах России перешла на использование цифровых радиостанций, работающих в стандарте APCO-25 (P25). В P25 данные передаются в цифровом виде со сжатием и кодами коррекции ошибок — это позволяет увеличить дальность устойчивой связи и больше каналов впихнуть в ту же полосу радиочастот. Также существует опциональная возможность шифрования переговоров, однако обычная полиция работает без шифрования.

Для приема P25-раций можно использовать декодер DSD. DSD ожидает аудиоданные на входе. Перенаправить аудио с SDRSharp в DSD можно с помощью Virtual Audio Cable. DSD весьма критичен к настройкам SDRSharp — я рекомендую устанавливать AF Gain около 20–40%, возможно отключать галочку Filter Audio. Если все идет по плану — в окне DSD побегут декодированные пакеты, а в наушниках будут слышны переговоры. Эта схема также работает с упомянутым плагином AutoTuner в SDRSharp.

Радиопереговоры самолетов и диспетчеров

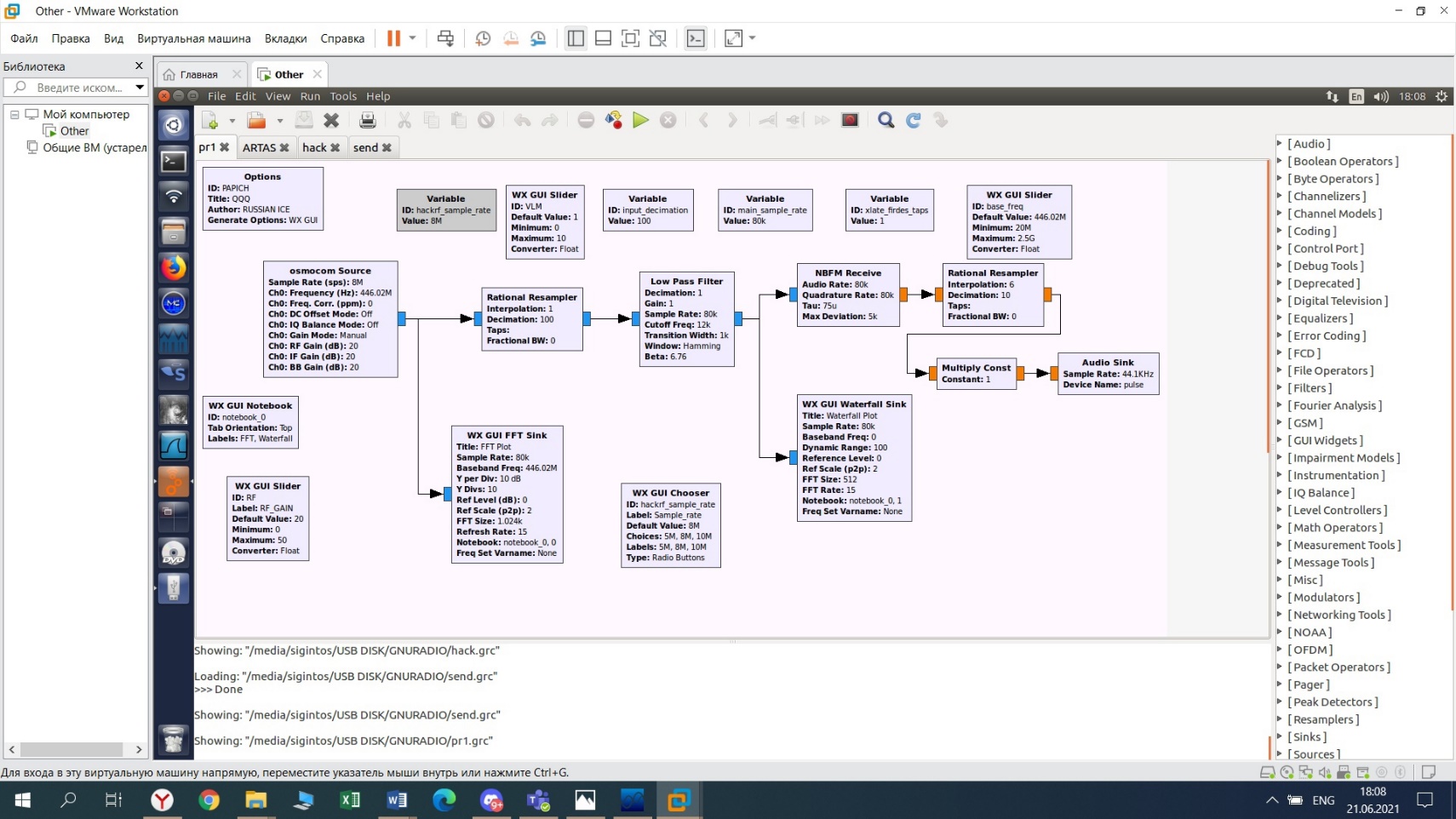
По историческим причинам для радиосвязи в авиации используется амплитудная модуляция. Обычно передачи с самолетов лучше слышно, чем от диспетчеров или погодных информаторов на земле. Диапазон частот — 117–130 МГц.

# 3 Анализатор спектра в Gnu Radio

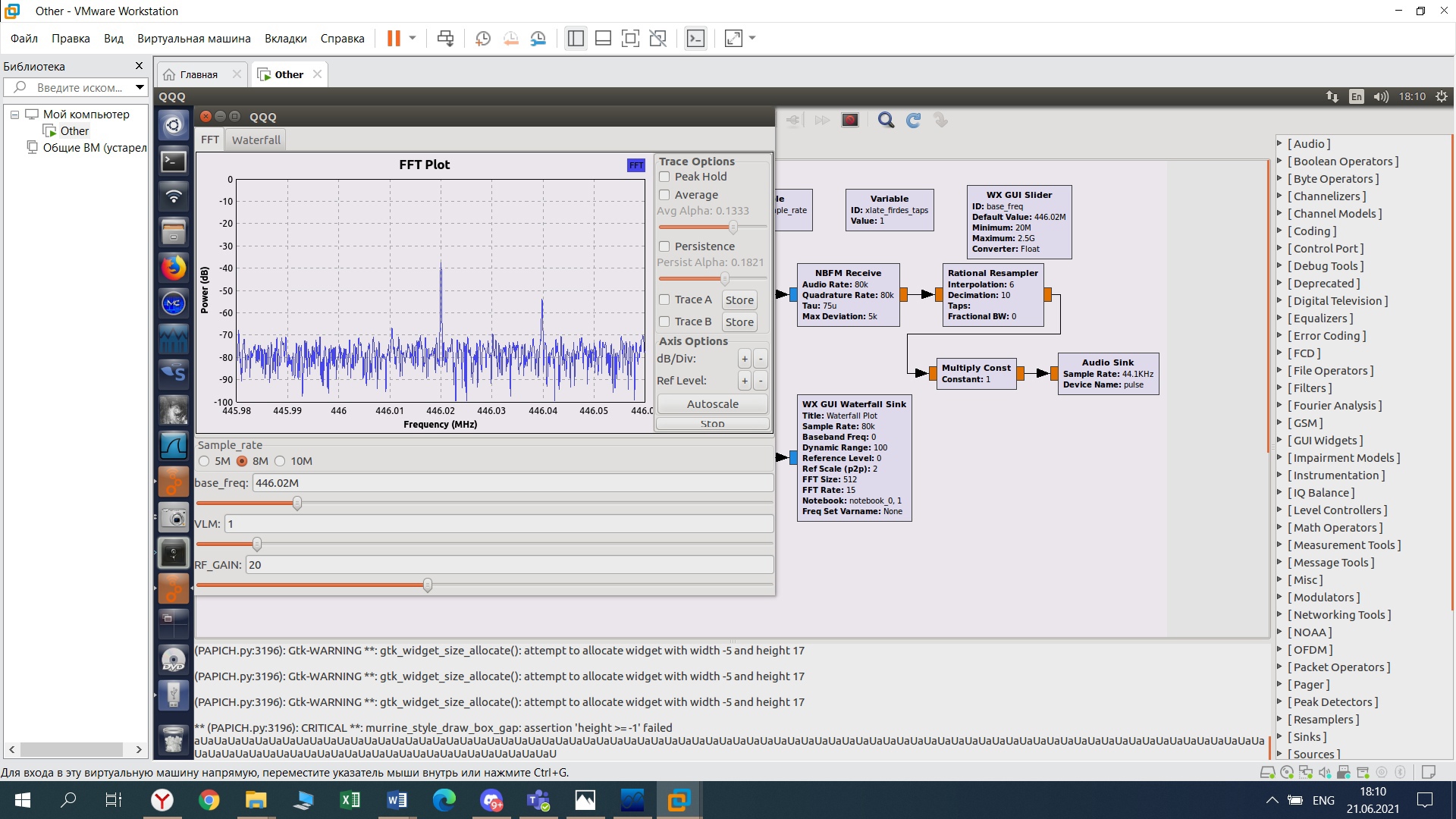
Для начала работы нужно установить SigintOS. В данной системе будет по умолчанию установлен пакет GNU Radio.

GNU Radio — это программный пакет, предназначенный для обработки данных, полученных от SDR-приемника, в реальном времени. Являющаяся стандартом де-факто для всех более-менее профессиональных забав в области радио, программа построена на модульной основе с учетом парадигмы ООП. Это настоящий радиоконструктор, в котором роль элементов отведена функциональным блокам: фильтрам, модуляторам/демодуляторам и несметному множеству других примитивов обработки сигналов. Таким образом, имеется возможность составить из них практически любой тракт обработки. Делается это в прямом смысле слова в несколько кликов мышкой в наглядном графическом редакторе, имя которому gnuradio-companion. Более того, gnuradio-companion написан на Python и позволяет генерировать схемы на Python. Но у такой гибкости есть и обратная сторона — освоить GNU Radio за десять минут невозможно.

Схема анализатора спектра выглядит следующим образом:



Пример его работы:



Если на определенной частоте наше устройство обнаружит сигнал, мы его увидим на графике. И дальше мы с помощью других программ, разработанных моей командой, можем записать сигнал и ретранслировать его для того, чтобы управлять какими-либо устройствами с радиоуправлением, либо же включить генератор помех для того, чтобы заглушить полезную передачу в данном канале.

# Заключение

Для достижения поставленной цели, в процессе прохождения учебной практики (учебно-лабораторного практикума) ознакомился с SDR-трансивером «HackRF», научился использовать необходимое дл работы ПО такое, как «SDRsharp» и «GNU Radio».

Также мной был разработан анализатор спектра, используя пакет Gnu Radio и написан отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

# Список использованных источников

1. SDR и HackRF для начинающих [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://hackware.ru/?p=8249 (дата обращения: 7.06.2021)
2. Делаем первые шаги с RTL-SDR [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://xakep.ru/2014/10/31/rtl-sdr-first-steps/ (дата обращения: 5.06.2021)