European Science Review 2024,
No 3–4.
ISSN 2310-5577

PREMIER Publishing
ppublishing.org

Section 3. Engineering science in general

DOI:10.29013/ESR-24-3.4-27-33

MODELING AND IMPLEMENTING SPOT JAMMING WITH GNU RADIO AND HACKRF ONE

Foziljonov Khojiakbar Ismail ogli [1]

[1] Department of Electronics and Radio Engineering, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Uzbekistan

Cite: *Foziljonov Kh.I. (2024). Modeling and Implementing Spot Jamming With Gnu Radio and Hackrf One. European Science Review 2024, No 3–4.* https://doi.org/10.29013/ESR-24-3.4-27-33

Abstract

This article presents the results of simulation of spot jamming in the GNU Radio environment using various modulating signals. In addition, experimental results of spot jamming using GNU Radio software in combination with HackRF One are presented.

Keywords: *spot jamming, GNU Radio, HackRF One, radio systems, electronic warfare, SDR, side electromagnetic radiation, modeling, modulation*

Introduction

Currently, spatial noise generators are used, as a rule, to mask informative side electromagnetic radiation and interference (SERI) of personal computers, workstations of computer networks and complexes at computer facilities (Liu, T., & Li, Y., 2019; Adamy, D. L., 2015; Foziljonov, K., & Fazil-janov, I., 2023). Various types of blockers can be used to suppress cellular communications that are not authorized to be used in radio microphone mode or in classrooms during an exam. Such devices are actually generators of barrage interference, blocking the frequency range of a particular cellular communication standard within a small radius. Both noise generators and signal jammers affect a wide range of frequencies, which can lead to restrictions on the use of legitimate radio communications, access to radio frequencies and wireless networks (Liu, T., & Li, Y., 2019).

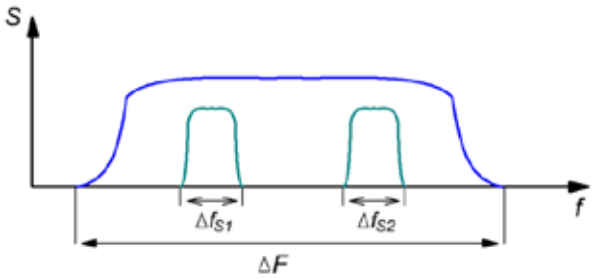
Spot jamming generators have less impact on the operation of authorized wireless technologies within a controlled area or room, since they have a relatively narrow frequency spectrum, commensurate with the bandwidth of the suppressed device. In addition, the continuous improvement of technical reconnaissance means, including in the direction of reducing the bandwidth of the frequencies used in order to reduce the likelihood of their detection, still leaves relevant issues of modernization and development of new circuits for narrow-band interference generators.

With the rapid development of communication technology, with the advantages of high flexibility, good compatibility, wide openness, and the ability to easily upgrade and expand the system at a later stage, soft radio technology has been applied to a variety of radio engineering activities, showing broad application prospects.

This paper discusses the modeling and experimental study of Spot jamming using GNU Radio software and the HackRF One radio device.

Radio-electronic interference is electromagnetic radiation that degrades the quality of operation of radio-electronic equipment, guided weapons, and information processing, reception and transmission systemsBased othe frequency range overlap, interference is divided into barrage and Spot jamming (SJ) (Schleher, D. C., 1999; Spezio, A. E., 2002).

Figure 1.

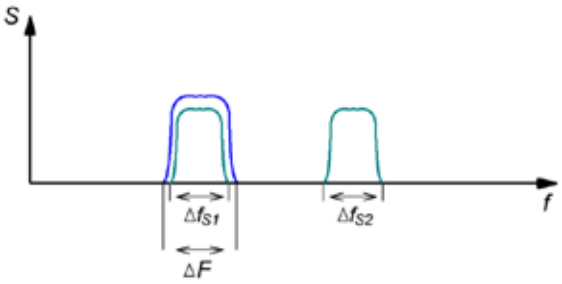


Barrier interference has a wide range of frequencies, many times greater than the bandwidth of the suppressed receiver (Fig. 1) (Schleher, D. C., 1999).

$$\Delta F \gg \Delta f_S.$$

Where ΔF – interference signal spectrum frequency; Δf_S – bandwidth of the suppressed receiver or signal.

Figure 2.



SJ has a relatively narrow frequency spectrum commensurate with the bandwidth of the suppressed device or a spectrum width commensurate with the signal spectrum width (Fig. 2) (Spezio, A. E., 2002).

$$\Delta F \approx \Delta f_S.$$

Simulation of Sj in the Gnu Radio Environment

GNU Radio is open source software that is a set of tools for developing software-defined radio (SDR) systems. It provides users with blocks (nodes) for signal processing that can be used to create various radio systems, ranging from conventional radio receivers to new generation communication systems ("Tutorials," GNU Radio, 21-Jul-2022; Miyashiro, H., Medrano, M., Huarcaya, J., & Lezama, J., 2017; Gummineni, M., & Polipalli, T. R., 2024).

With GNU Radio, users can develop their own radio systems using flexible and powerful signal processing tools.

GNU Radio is widely used in both academic research and commercial projects, including prototyping, educational purposes, and scientific research.

GNU Radio's core capabilities include signal processing, filtering, modulation, demodulation, encoding and decoding, and interfacing with various hardware devices via standard interfaces such as USB and Ethernet.

In this article, two types of modulation AM and FM were chosen for the formation of

modulated PPs. Below are the AM PP simulation model (Fig. 3) (Harianto, B. B., Rifai, M., Irfansyah, A., & Suprapto, Y., 2021; Bhimavaram, K. R., Hiremath, P. S., & Kumar, S. A., 2021). In Fig. Figure 4 shows the spectrum of the AM PP, in this case, a harmonic signal is used as a modulating signal.

Figure 3.

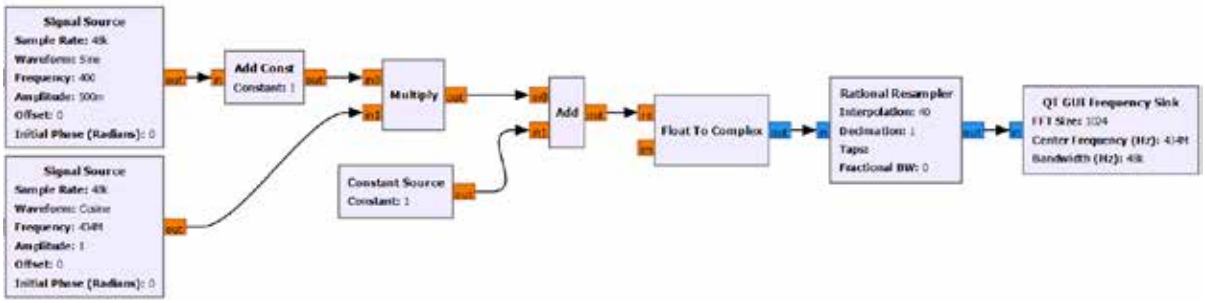
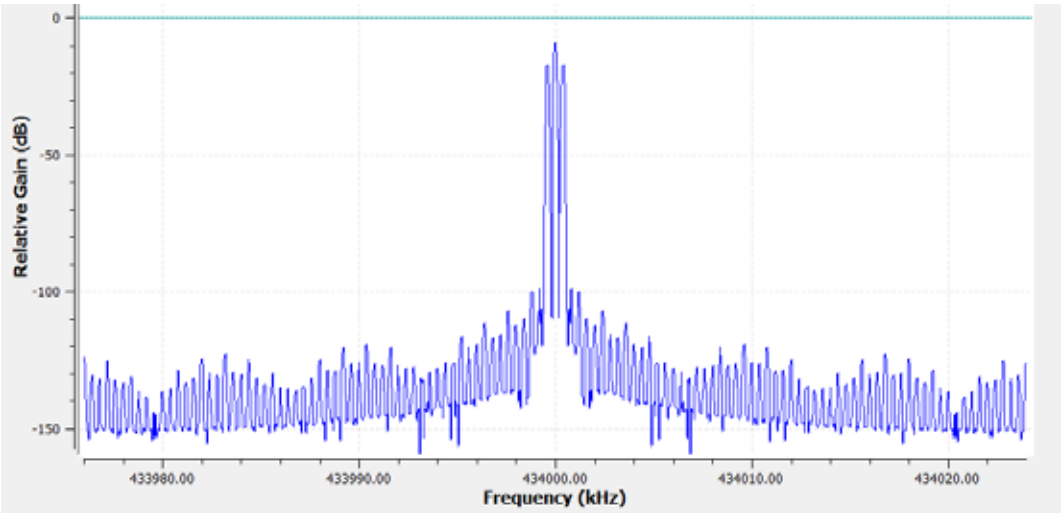


Figure 4.



Replacing the signal source block with Wav file source makes it possible to use an audio file as a modulating signal. The result of the simulation, the spectrum of the AM SJ is shown below (Fig. 5).

Figure 5.

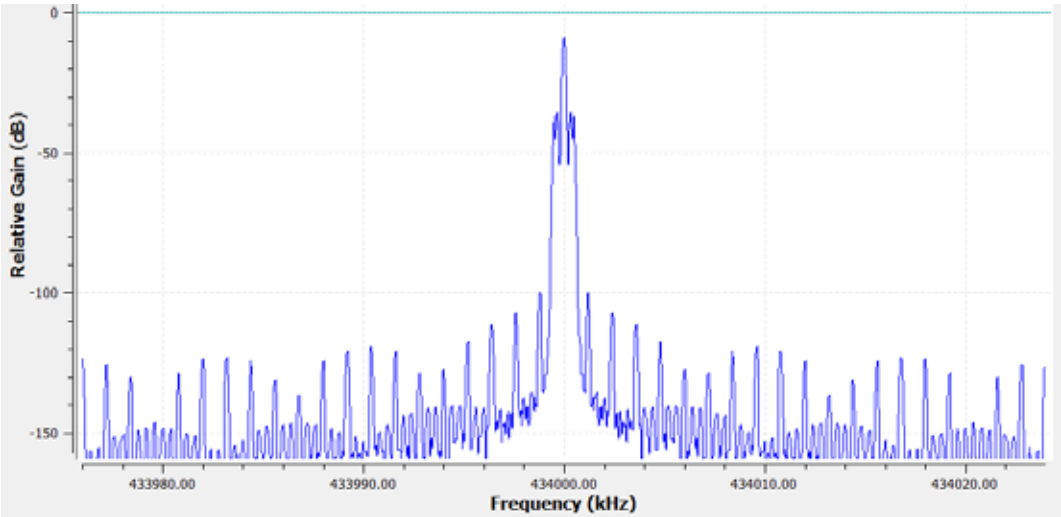
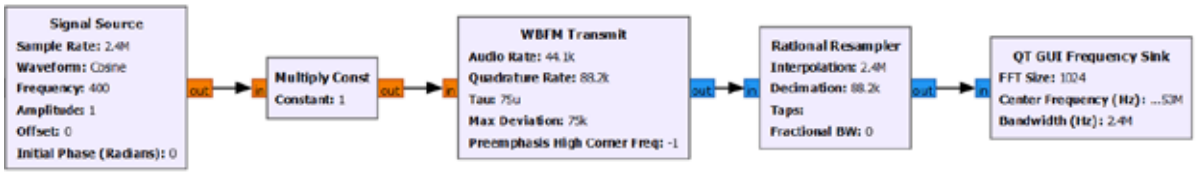


Figure 6.



In GNU Radio, the WBFM Transmit block is provided to generate an FM signal. This block generates wideband frequency modulation (Shrivastava, A., 2018; Martoyo, I., Setiasabda, P., Kanalebe, H. Y., Uranus, H. P., & Pardede, M., 2018; Gummineni, M., & Polipalli, T. R., 2020). By connecting the corresponding blocks, we can obtain a simulation model of the FM SJ (Fig. 6).

In Figure 7 shows the oscillogram and spectrum of the FM SJ. In this case, a harmonic signal is used as a modulating signal.

Figure 7.

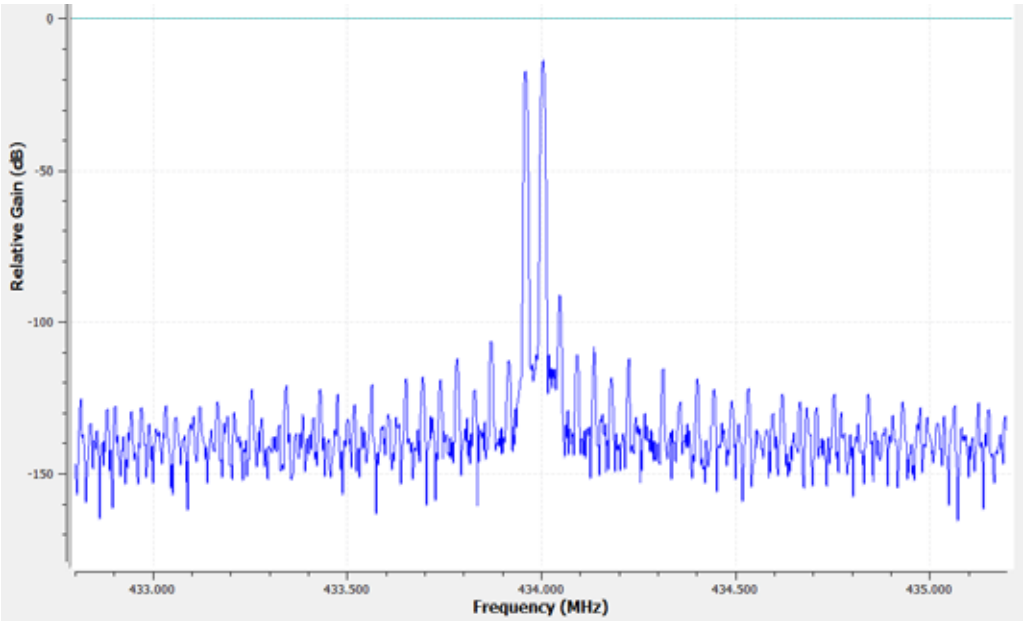


Figure 8.

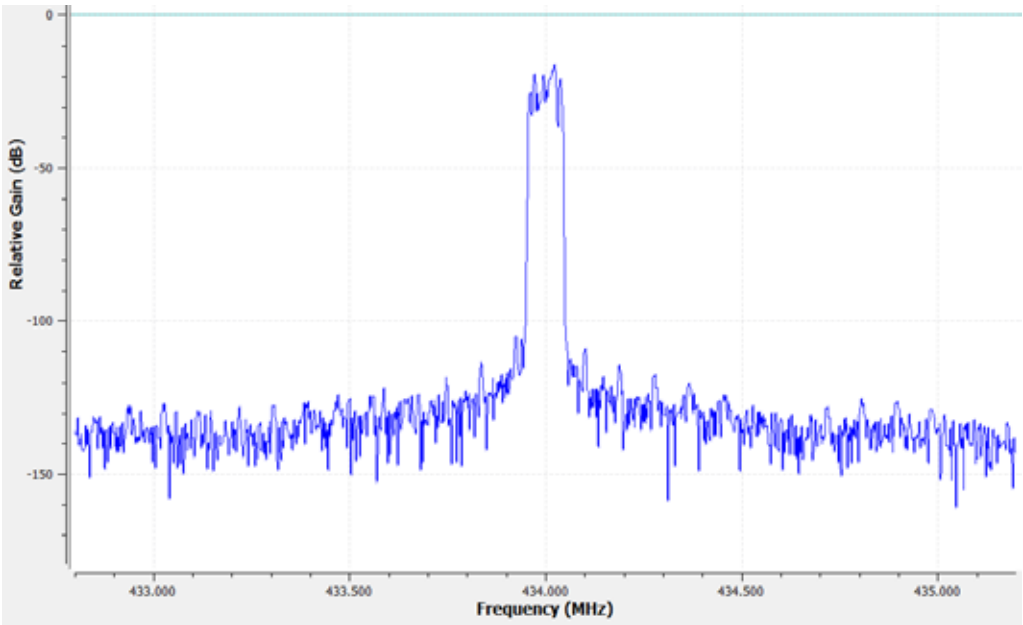


Figure 8 shows the result of the simulation, where an audio file is used as a modulating signal.

Experimental Part

This section presents the results of AM and FM PP radiation. In the models shown in Figures 3 and 6, by replacing the QT_GUI_Frequency_Sink blocks with an Osmocom sink, it becomes possible, using the HackRF One SDR transceiver and the ANT500 antenna (Gummineni, M., & Polipalli, T. R., 2020; Davronbekov, D., & Fozilzhonov, H., 2021; SDRuno User Manual v 1.41. SD Rplay, 21-Jul-2020), to broadcast (radiate) the generated SJs at a frequency of 434 MHz.

Figure 9. *Spectrum of the FM SJ signal using an audio file as a modulating signal*

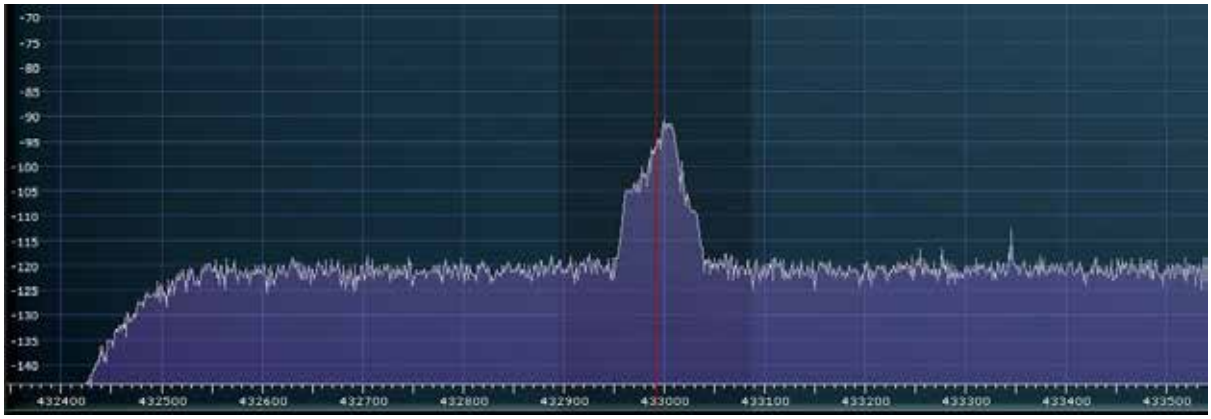


Figure 10. *Spectrum of the FM SJ signal, a harmonic signal is used as a modulating signal*

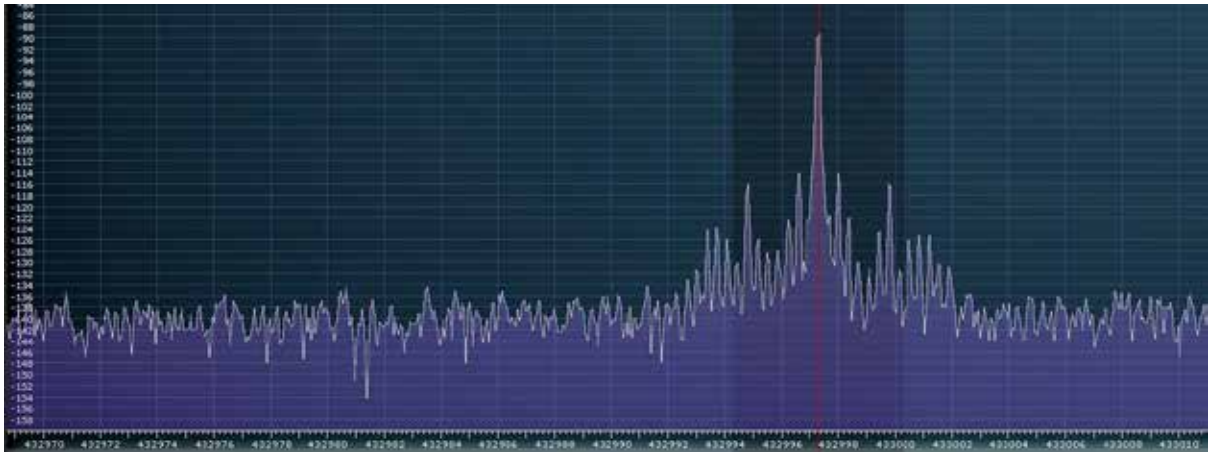
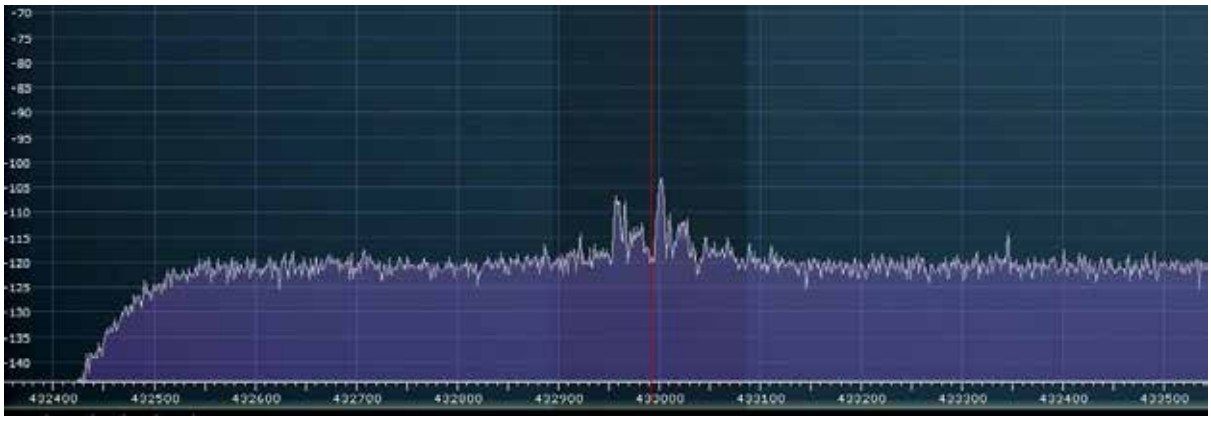


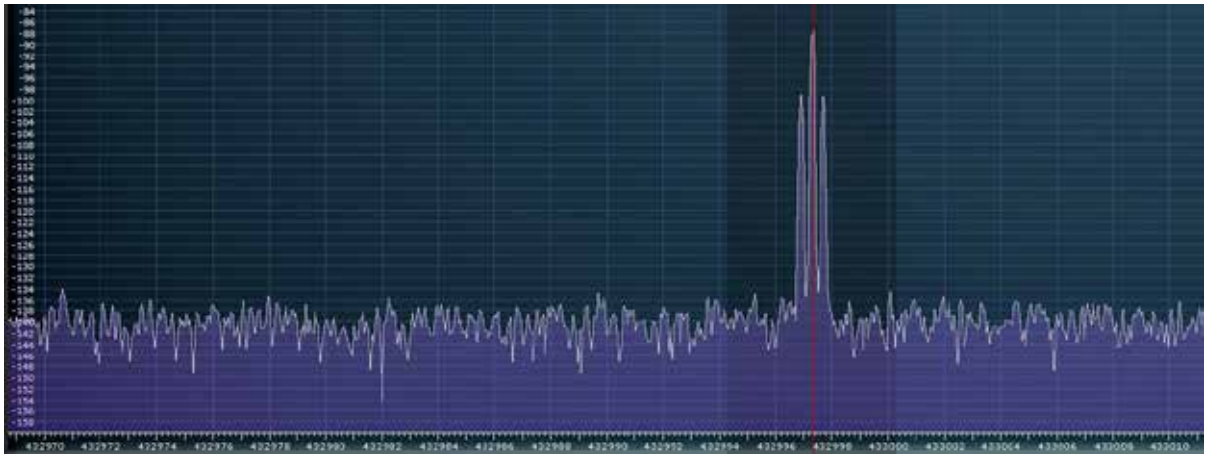
Figure 11. *Spectrum of an AM SJ signal using an audio file as a modulating signal*



The SDRplay RSPdx with the SA-7000 antenna and the SDRuno program for working with the SDR receiver were used as an SDR receiver.

Figures 9–12 show the spectrum of the emitted SJ. In Figure 9, an audio file is used as a modulator.

Figure 12. *Spectrum of an AM PP signal, a harmonic signalis used as a modulating signal*



Thus, based on the results of the experiment and simulation, the following conclusions can be drawn:

GNU Radio software allows you to create simulation models for generating modulated targeted interference with different modeling signals and frequencies. This makes it possible to study the effects of such interference on radio systems or electronic devices without the risk of damaging the actual equipment.

Using HackRF One in combination with GNU Radio, targeted interference can be transmitted at various frequencies. It is important to note that the interference power will be limited by the maximum output power of the HackRF One. This approach has a wide range of applications, including testing the immunity of radio systems to interference, evaluating the effectiveness of interference detection and suppression algorithms, and in radio frequency attacks to disrupt radio systems.

The results obtained can be used to demonstrate targeted interference to military and radio engineering students. In addition, it is possible to use targeted interference to disguise SERI or to disrupt synchronization in reconnaissance receivers.

References

Liu, T., & Li, Y. (2019). Electromagnetic Information Leakage and Countermeasure Technique: Translated by Liu Jinming, Liu Ying, Zhang Zidong, Liu Tao. Springer.

Adamy, D. L. (2015). EW 104: electronic warfare against a new generation of threats. Artech House.

Foziljonov, K., & Faziljanov, I. (2023). Active methods and means of information protection against leakage through channels of side electromagnetic radiation and interference. Science and innovation,– 2(A4).– P. 46–52.

Schleher, D. C. (1999). Electronic warfare in the information age. Artech House, Inc.

Spezio, A. E. (2002). Electronic warfare systems. IEEE Transactions on Microwave Theory and Techniques,– 50(3).– P. 633–644.

Лихолоб П. Г., Буханцов А. Д., Девицына С. Н., & Курлов А. В. (2015). Модель прицельной узкополосной помехи. Экономика. Информатика,– 36 (19 (216)).– P. 191–196.

“Tutorials,” GNU Radio, 21-Jul-2022. [Online]. Available: https://wiki.gnuradio.org/index.php/Tutorials. (Accessed: 8-March-2023).

Miyashiro, H., Medrano, M., Huarcaya, J., & Lezama, J. (2017, August). Software defined radio for hands-on communication theory. In 2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON) (P. 1–4). IEEE.

Gummineni, M., & Polipalli, T. R. (2024, January). Implementation of software-based communication system using SDR and GNU radio. In AIP Conference Proceedings (Vol. 2512, No. 1). AIP Publishing.

Harianto, B. B., Rifai, M., Irfansyah, A., & Suprapto, Y. (2021, March). Design Indoor FM Communication Based on SDR and GNU Radio Using Validated Spectrum Analyzer. In Journal of Physics: Conference Series (Vol. 1845,– No. 1.– 012078 p). IOP Publishing.

Bhimavaram, K. R., Hiremath, P. S., & Kumar, S. A. (2021, September). Remote labs for communications. In Online engineering and society 4.0: proceedings of the 18th international conference on remote engineering and virtual instrumentation (Vol. 298).

Shrivastava, A. (2018). Design and development of low-range frequency modulated signal (FM) transmitter. BIBECHANA,– 15.– P. 30–36.

Martoyo, I., Setiasabda, P., Kanalebe, H. Y., Uranus, H. P., & Pardede, M. (2018, December). Software defined radio for education: Spectrum analyzer, fm receiver/transmitter and gsm sniffer with hackrf one. In 2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME) (P. 188–192). IEEE.

Gummineni, M., & Polipalli, T. R. (2020). Implementation of reconfigurable transceiver using GNU Radio and HackRF One. Wireless Personal Communications,– 112(2).–P. 889–905.

Давронбеков, Д., & Фозилжонов, Х. (2021). Сравнительный анализ программно-определяемых радиосистем для исследования побочных электромагнитных излучений и наводок. InterConf,– С. 415–419.

SDRuno User Manual v 1.41. SD Rplay, 21-Jul-2020. [Online]. Available: https://www.sdrplay.com/help/ (Accessed: 13-May-2023).

Ogli, F. K. I. (2021, November). Study of the Spectrum of Side Electromagnetic Radiations of Video Interface DVI. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (P. 1–3). IEEE.

Abdimuratov Z. S., Manbetova Z. D., Imankul M. N., Chezhimbayeva K. S., Davronbekov D. A. Absorbers of electromagnetic radiation based on shungite species // News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, 2021.– 1(445).– P. 6–12. URL: https://doi.org/10.32014/2021.2518-170X.11

Tuychiyev B. O., Davronbekov D. A. Models and algorithms for the optimal processing of spatio-temporal signals by the method of fractal // 2020 International Conference on Information Science and Communications Technologies, ICISCT 2020.

Davronbekov D. A., Abdimuratov Z. S., Manbetova Z. D. Measurement of Electromagnetic Radiation Levels from Mobile Radiotelephones // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities. ICISCT 2019. DOI: 10.1109/ICISCT47635.2019.9012052

submitted 06.04.2024;
accepted for publication 24.04.2024;
published 28.05.2024

Contact: foziljonov.x.i@gmail.com