DOI: https://doi.org/10.36719/2663-4619/114/269-275

Asad Rustamov
Azerbaijan Technical University
https://orcid.org/0009-0002-3080-8409
asadrustamov1122@gmail.com
Tofig Bakhshiyev
Azerbaijan Technical University
Master student
https://orcid.org/0009-0002-3650-246X
baxshiyevtofiq@gmail.com

Artificial Intelligence Integrated Software-Defined Radio Antennas for Anti-Drone Applications

Abstract

There has been a marked surge in unmanned aerial vehicle (UAV) usage, raising serious concerns about intrusions into restricted or sensitive airspace. The goal of this article is to show AI-powered SDR antennas designed to cover multiple frequency bands, enabling real-time identification and targeted interference or jamming of unauthorized UAV signals. Software-defined radio (SDR) technologies, particularly when augmented with artificial intelligence (AI), have emerged as highly adaptable and relatively low-cost platforms for detecting, classifying, and neutralizing rogue drones. Several topics have been researched including implementation challenges, limited processing capabilities on edge devices, potential vulnerabilities in radio frequency (RF) channels, and ensuring robust AI classification despite evolving signal characteristics and adversarial spoofing attempts. Collaborative or distributed SDR solutions are proposed to enhance detection accuracy by aggregating RF data from multiple vantage points, thereby overcoming individual sensor constraints. As a result of research it has been found that ongoing studies in sensor fusion, antenna design, and edge AI optimization is expected to further enhance the capabilities of these systems, providing robust and adaptable defense against unauthorized drones

Keywords: *artificial intelligence, software, radio, antenna, drone, frequency*

Əsəd Rüstəmov
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0002-3080-8409
asadrustamov1122@gmail.com
Tofiq Baxşıyev
Azərbaycan Texniki Universiteti
magistrant
https://orcid.org/0009-0002-3650-246X
baxshiyevtofiq@gmail.com

Dron əleyhinə tətbiqlər üçün süni intellekt inteqrasiyalı proqram təminatlı radio ilə işləyən antenalar

Xülasə

Məhdud və ya həssas hava məkanına müdaxilələrlə bağlı ciddi narahatlıqlar yaradan pilotsuz uçuş aparatlarının (PUA) istifadəsində nəzərəçarpacaq artım olub. Bu məqalənin məqsədi real vaxt rejimində identifikasiyaya və icazəsiz PUA siqnallarının müdaxiləsinə imkan verən çoxsaylı tezlik diapazonlarını əhatə etmək üçün nəzərdə tutulmuş süni intellektlə işləyən proqram təminatı ilə müəyyən edilmiş radio antenalarını araşdırmaqdır. Proqram təminatı ilə müəyyən edilmiş radio texnologiyaları, xüsusən də süni

intellekt ilə genişləndirildikdə, yalançı yaradılmış dronları aşkar etmək, təsnif etmək və zərərsizləşdirmək üçün yüksək uyğunlaşa bilən və nisbətən ucuz platformalar kimi ortaya çıxır. Tətbiq problemləri, kənar cihazlarda məhdud emal imkanları, radiotezlik kanallarında potensial zəifliklər təhlil edilmişdir. Təsir edən siqnal xüsusiyyətlərinə və rəqib saxtakarlıq cəhdlərinə baxmayaraq möhkəm süni intellekt təsnifatının təmin edilməsi də daxil olmaqla bir neçə mövzu tədqiq edilmişdir. Nəticədə, bir çox mənbədə radio tezlik məlumatlarını birləşdirərək aşkarlama dəqiqliyini artırmaq və bununla da fərdi sensor məhdudiyyətlərini aradan qaldırmaq üçün birgə və ya paylanmış proqram təminatı ilə müəyyən edilmiş radio texnologiya avadanlıqlarının tətbiqi göstərilmişdir.

***Açar sözlər**: süni intellekt, proqram təminatı, radio, antena, dron, tezlik*

Introduction

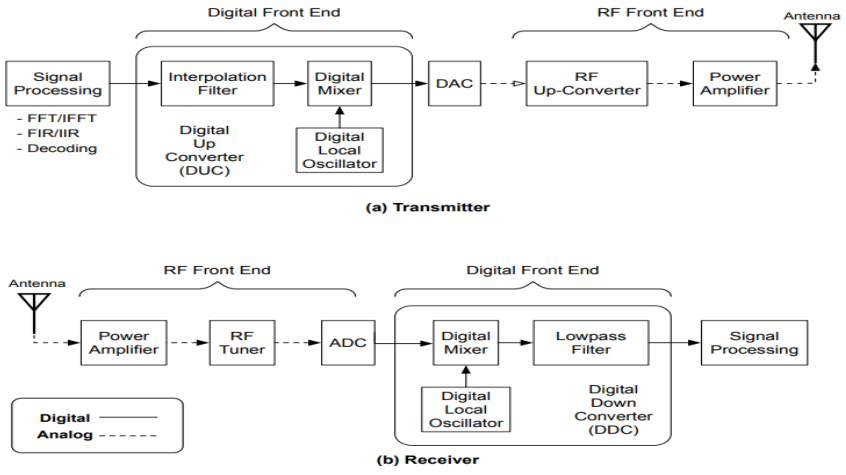
The use of drones in various fields is increasing, but their misuse in sensitive areas has increased the need for effective counter-UAV systems. Traditional detection methods based on fixed thresholds or static hardware cannot cope with the dynamic and evolving nature of UAV transmissions (Flak, 2021). For example, in a military scenario, the needs of these platforms change in light of the challenging conditions encountered during the mission, which leads to the development and use of new protocols that were not foreseen at the time of the initial design (Akeela & Dezfouli, 2018). Additionally, small-size UAV neutralization with shooting from air missile systems is not suitable for governments. This challenge makes continuous developments in radio electronic combat methods, and anti-drone techniques crucial (Rustamov et al., 2024). This article aims to present software and security parts of SDR systems. Section 1 describes architecture samples of SDR systems. Section 2 describes AI integrations and cyber security perspective of this field. Section 3 shows what kind of drone detection techniques can be implemented. The last section which is section 4 demonstrates future research directions. Software-defined radio (SDR) offers an alternative by allowing real-time reconfiguration of scan parameters and fast signal processing (Sinha et al., 2016). SDRs are implemented using various types of hardware platforms, such as General Purpose Processors (GPP), Graphical Processing Units (GPU), Digital Signal Processors (DSP), and Field Programmable Gate Arrays (FPGA). General structure of SDRs includes the following components: antenna, radio frequency front-end, analog-to-digital converter, digital-to-analog converter, digital front-end. Many important processes, including digital signal processing, channel selection, modulation, and demodulation, occur in the digital front-end. The superficial sequence of processes at the sending and receiving ends of the signal is as follows:

Transmitter: Generates a baseband signal, converts it to an intermediate frequency, then converts it to radio frequency, and sends it through an antenna.

Receiver: Amplifies the incoming radio frequency, converts it to an intermediate frequency, digitizes it with an analog-to-digital converter, mixes it down to baseband, filters it, and cuts it, then demodulates and decodes it.

This stage is usually handled by dedicated hardware such as an Application Specific Integrated Circuit (ASIC), FPGA, or DSP. Generalized architecture of SDRs is shown in figure 1.

Figure 1 (Generalized SDR architecture) (Akeela & Dezfouli, 2018)



Research

1. SDR architecture for drone defense

1.1 Wideband Monitoring and Data Acquisition

Drone detection sensors capture initial I/Q samples from a wide range of frequencies, typically spanning the 2.4 GHz and 5 GHz ISM bands, to continuously monitor UAV signals (Flak, 2021). High-speed analog-to-digital converters (ADCs) and tunable RF front-ends ensure that SDR systems have adequate range and resolution for real-time signal acquisition (Sinha et al., 2016). Field-programmable gate arrays (FPGAs) are used to compress the initial spectral data into frames before the data is transmitted for further processing. Sensor based FPGAs will be more efficient by incorporating fast Fourier transforms into signal processing, will be able to sense a wider bandwidth in the 2.4 GHz ISM band (up to 83 MHz), and will be able to send SDR frequency domain signals instead of time domain signals. Figure 2 presents proposed sensor architecture with FPGA.

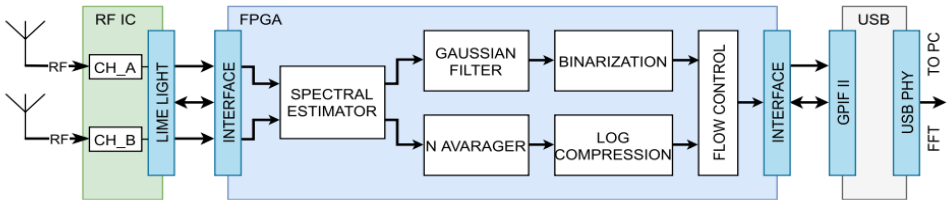


Figure 2 (sensor architecture based on SDR with extended FPGA) (Flak, 2021)

Main concept is to obtain spectrogram from I/Q samples. Input signal is segmented and then Short Time Fourier Transform is conducted. Mathematically, discrete form of STFT is like:

$$STFT \equiv X(m,\omega) = \sum_{n=-\infty}^{\infty} x[n]w[n-m]e^{-j\omega n}$$

Where: x[n] is the discrete-time signal (your drone's RF sample), w[n-m] is the window function, n is sample index, m indicates the position of the analysis window in the time dimension, ω is angular frequency for the discrete transform (Flak, 2021).

1.2 Software-based signal processing

MATLAB-based signal processing software is presented which implements a hybrid Mini/Micro UAV detection method using ADALM-PLUTO SDR hardware. In order to differentiate real threats from Wi-Fi-based drones or disturbances, Wi-Fi signals are first decoded. Then, using maximum-value-holding or averaging modes, an FFT converts time-domain samples into the frequency domain. The noise floor is then established using a histogram-based method, and the detection threshold is set by a user-defined offset. Calculations of bandwidth and center-frequency are then made possible by comparing FFT bins to this threshold in order to detect signals. By fine-tuning overlapping signals, a pulse-on-pulse (PoP) technique enhances center-frequency estimation. The findings of Wi-Fi decoding, threshold-based detection, and overlapping signal identification are then combined in an interference signal discrimination step, which successfully eliminates non-UAV signals. This software layer replaces static threshold detection methods with dynamic algorithms that adapt detection parameters based on the evolving radio environment (Özkaner & Akça, 2024).

If the code would be written in python, then the estimated conceptual structure would be like following: Python SDR interfaces (e.g., SoapySDR, pyuhd) are used to set frequency, gain, and sampling rate. I/Q samples are captured into arrays in the code. FFT or spectrogram computations are performed with respective libraries (NumPy FFT, PyFFTW). Signals above threshold are identified, bandwidth and center frequency is calculated. Detect overlapping signals (e.g., Pulse-on-Pulse algorithms). Decode known protocols (e.g., Wi-Fi) to remove them or mark them as non-UAV. Finally, the results are logged or visualized, highlighting signal parameters and classifications

2 AI integrating into SDR and Cyber Security perspective

2.1 Detection of UAV signal

While there are many drone signal detection methods like radar, camera and radio frequency scan based, 1 of them is noteworthy. Edge-DF is specialized directional detector designed for detecting drones. Its 4 band and sector antenna that is configured as 4x4 makes long range detection possible. Additionally, it uses AI-based object recognition and Full Channel parallel reception technology to accurately detect and identify drone signals as well as their direction. Furthermore, EdgeDF provides direction finding and 360-degree multiple drone detection with less weather interference than previous systems (Ki et al., 2023).

2.2 Adaptive countermeasures

Multiple classifiers can be integrated into a single decision-making system using ensemble learning techniques like XGBoost and K-Nearest Neighbor (KNN) algorithms, which improves the detection mechanism's general endurance and reliability. SDR controlled UAV countermeasures like BladeRF x40 can deceive GPS systems seamlessly integrating real-time sensor inputs (LIDAR, accelerometers, magnetometers) to redirect drones toward forced landing sites (Michailidis et al., 2024). Another tested idea is “Security Monitor” software that works between hardware and OS. In SM two USRP2 SDR devices are used, one being as transmitter and another as receiver. Transmitter sends instructions about technical parameters and the receiver receives them. If SM software detects any parameter altered it blocks the signal. The “correct” parameters are sent by the transmitter in each instance, and the SM compares them to the actual parameters that the OS or application is sending to the hardware. The OS marks a discrepancy in its parameters as an assault. Because SDRs are so adaptable, rogue code in the operating system may rearrange frequencies, boost power, or falsify sensing data, leading to interference or unauthorized broadcasts. Since the SM 'hooks' at the hardware level and checks parameters against the transmitter's instructions before finalising them at the hardware level, it may still impose policy even in the event that the OS is compromised (Li et al., 2018).

2.3 Security and resource management

From security perspective it can be said that there are specific types of attack that can be conducted and they are: frequency change attack, power change attack, sensing frequency attack (Li et al., 2018). Additionally there are sensor and signal spoofing attacks that must be taken into account. In sensor spoofing attack the attacker sends various fake sensor values to controller of UAV. Then UAV gets stuck in feedback loop which can even lead to total management loss. Security Code Estimation and Replay is one type of signal spoofing attack where attacker estimates each symbol of secret code. In order to recreate the secret code, the symbol estimate is updated constantly by monitoring the received signal and concurrently employed in the spoof signal. The fake signal is then transmitted to the real signal with a slight delay (Chamola et al., 2021).

3. Drone detection strategies

3.1 Detection of drone

Angle of arrival (AoA) and phase difference techniques are used by SDR systems to detect position of UAV. DronEnd UAV detection system is part of DronEnd research project and consists of defense agent drone, depicted in black, on which a USRP E312 stand-alone SDR platform is mounted. Basically one drone detects, localizes and defends against another drone (Chiper et al., 2022).

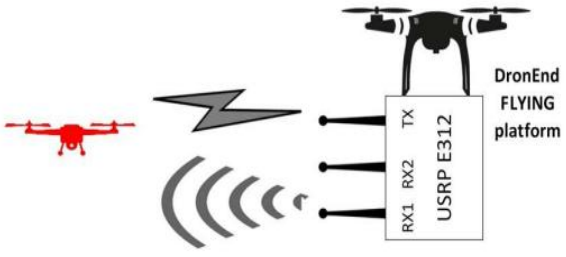


Figure 3 (DronEnd FLYING platform) (Chiper et al., 2022)

3.2 Building comparison graph based on literature data with MATLAB

The literature in (Flak, 2021) shows benefits of building FPGA on the LimeSDR-USB board, which performs Fast Fourier Transform and pre-filtering so that only 12-bit frequency domain samples or even binarized data capturing an 83 MHz are sent over USB. This reduces the data rate from approximately 250MB/s (which can overload standard USB interfaces) to 125MB/s first after FFT filtering, and then to 10MB/s after binarization, making real-time drone detection possible even on low-power processors. Most importantly, the original SDR protocol remains intact and provides minimal changes to existing software workflows.

To verify and visually illustrate these, we developed a MATLAB script that generates a graph which is comparing the three data rate stages. Figure 4 (shown below) presents that the proposed FPGA-based processing and binarization dramatically lower the data throughput, making real-time processing on low-power systems feasible.

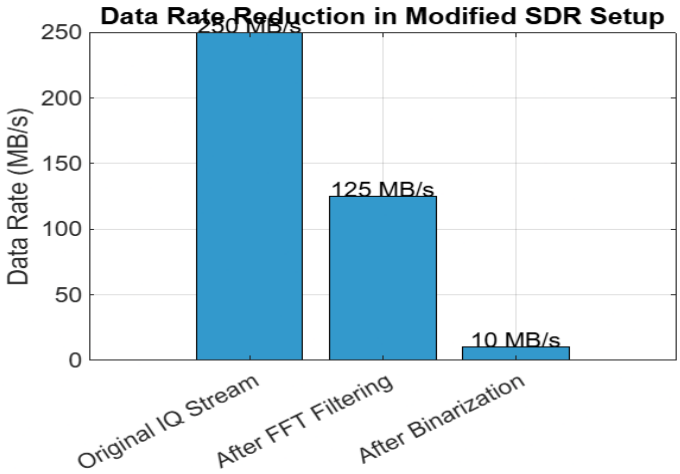


Figure 4 (Comparison graph that show data rate reduction in modified SDR)

3.3 Radio frequency jamming, and spoofing

Primary UAV operation modes: Many drones use 2.4 GHz or 5.8 GHz for manual remote control. Autonomous flight however, relies on GNSS (GPS) signals for navigation (Ferreira et al., 2022). Besides, there are also ground control station method that is also program or software based (Rustamov et al., 2024). Because the drone's flight mode is not always known, the system jams both the remote-control frequencies and GNSS signals. There are various techniques of jamming including: barrage, sweep, tone, successive pulses, protocol-aware, smart, GNSS, tone and others (Ferreira et al., 2022) (Ferreira et al., 2020) (Chamola et al., 2021). The authors in (Ferreira et al., 2020) and (Chamola et al., 2021), discuss all of the mentioned jamming techniques in detail. Civil GPS lacks encryption or authentication, making it easy to transmit fake signals that mimic legitimate satellite broadcasts. By faking GPS signals as if they were from real satellites, a drone receiver can be tricked into following the path set by the faker (Chamola et al., 2021).

4. Future research directions

4.1 Distributed SDR Networks

Future anti-drone systems may benefit from deploying distributed SDR nodes that share partial classification information over secure channels to improve overall detection accuracy (Flak, 2021). This will save time and hardware costs.

4.2 Time synchronization in SDR systems

Recent research which is conducted by (Rustamov et al., 2025) has shown that using the time factor to shorten transmission times can improve the coordination of the operation of several radio-electronic devices including SDRs. The author also mentions that a time regulation device which dynamically modifies the repetition frequency across several radar units is a promising method for reducing asynchronous interference.

4.3 Antenna and radio frequency "Front-End" design

In (Sinha et al., 2016), the authors focus on challenges related to MIMO systems and tunable reconfigurable antennas that provide uniform performance and efficient power transfer across multiple bands. While this is being researched and developed, for notifying the importance of this issue example block diagram is being presented. The figure below demonstrates the Multiple-Input Multiple-Output (MİMO) enabled SDR system.

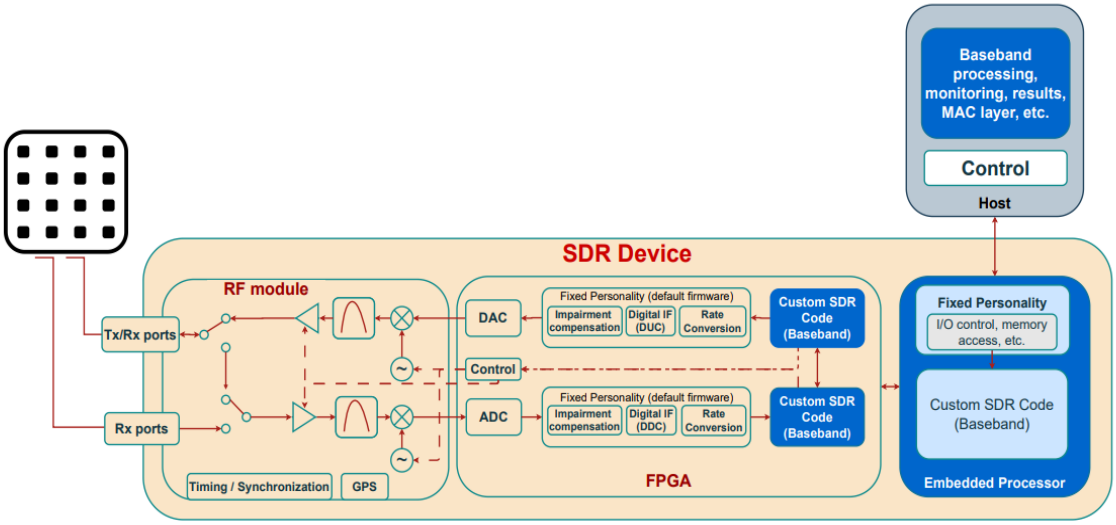


Figure 5 (FPGA-integrated SDR with MIMO capabilities) (Michailidis et al., 2024)

4.4 SDR on container

Building SDR environment on containers is feasible from IT and cyber security point of view. Containers are latest virtualization technology that use directly the kernel of OS. They are faster and use less resource than legacy virtual machines. Container technology work better in cloud environments and many dominant telecommunication providers build their virtual environment with containers. The authors in (Mehr et al. 2023) explain how containers work.

Protocol like Automatic Dependent Surveillance-Broadcast (ADS-B) and LoRa decoding service can be deployed with docker-compose files (Machado et al., 2023).

Conclusion

AI-powered SDR antennas offer a promising and cost-effective solution for counter-UAV operations. By utilizing broadband monitoring, real-time spectral analysis, and AI-driven adaptive jamming or spoofing, these systems overcome many of the limitations associated with traditional anti-drone technologies. However, challenges remain in ensuring secure, efficient processing on resource-constrained platforms and reliable operation in dynamic spectral environments. Ongoing research in distributed sensor fusion, advanced antenna design, and edge AI optimization is expected to further enhance the capabilities of these systems, providing robust and adaptable defense against unauthorized drones. Besides, implementing SDR systems in containers will be efficient from an IT and cyber security point of view.

References

1. Akeela, R. və Dezfouli, B. (2018). Software-defined radios: Architecture, state-of-the-art, and challenges. *Computer Communications*, 128, 106-125. https://doi.org/10.1016/j.comcom.2018.07.012
2. Chamola, V., Kotesh, P., Agarwal, A., Naren, Gupta, N. və Guizani, M. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Networks*, 111, 102324. https://doi.org/10.1016/j.adhoc.2020.102324

3. Chiper, F.-L., Martian, A., Muscalu, D.-I., Vladeanu, C. və Marghescu, I. (2022). Aerial Drone Defense System Based on Software Defined Radio Platforms. *14th International Conference on Communications (COMM)*.
4. Ferreira, R., Gaspar, J., Sebastião, P. və b. (2020). Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. *Wireless Personal Communications*, 115, 2705–2727. https://doi.org/10.1007/s11277-020-07212-6
5. Ferreira, R., Gaspar, J., Sebastião, P. və Souto, N. (2022). A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. *Sensors*, 22(4), 1487. https://doi.org/10.3390/s22041487
6. Flak, P. (2021). Drone Detection Sensor with Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform. *IEEE Access*, 9, 114574–114586.
7. Ki, Y., Chun, S. və Ryoo, J. (2023). ADS: Study on the Anti-Drone System: Today's Capability and Limitation. *Proceedings of the 14th International Conference on Information and Communication Technology Convergence (ICTC)*, 387–392. https://doi.org/10.1109/ICTC58733.2023.10392984
8. Ki, Y., Chun, S. və Ryoo, J. (2023). Study on the Anti-Drone System: Today's Capability and Limitation. *Proceedings of the 14th International Conference on Information and Communication Technology Convergence (ICTC)*, 387979–8.
9. Li, K., Yu, X., Zhang, H., Wu, L., Du, X., Ratazzi, P. və Guizani, M. (2018). Security Mechanisms to Defend against New Attacks on Software-Defined Radio. *Proceedings of the IEEE International Conference on Computing, Networking and Communications (ICNC)*. https://doi.org/10.1109/ICCNC.2018.8390381
10. Machado, E.R., Feldman, M. və Müller, I. (2023). A Container-based Architecture to Provide Services from SDR Devices. *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, 1–6. https://doi.org/10.1109/INDIN51400.2023.10217954
11. Mehr, I.E., Minetto, A., Dovis, F., Pica, E., Cesaroni, C. və Romano, V. (2023). An Open Architecture for Signal Monitoring and Recording Based on SDR and Docker Containers: A GNSS Use Case. *IEEE EUROCON 2023 – 20th International Conference on Smart Technologies*, 66–71. https://doi.org/10.1109/EUROCON56442.2023.10199078
12. Michailidis, E.T., Maliatsos, K. və Vouyioukas, D. (2024). Software-Defined Radio Deployments in UAV-Driven Applications: A Comprehensive Review. *IEEE Open Journal of Vehicular Technology*, 1–10. https://doi.org/10.1109/OJVT.2024.3477937
13. Özkaner, A. və Akça, Y. (2024). Mini/Micro UAV Detection in the Presence of ISM or Spurious Signals and an Experimental Application on an SDR. *Engineering Science and Technology, an International Journal*, 49, 101591. https://doi.org/10.1016/j.jestch.2023.101591
14. Rustamov, A., Hashimov, E., Ganjiyev, A., Rahimli, V. və Hashimov, R. (2025). System technical solution of electromagnetic adaptation. *Advanced Information Systems*, 9(1), 86. https://doi.org/10.20998/2522-9052.2025.4.10
15. Rustamov, A. R., Gasanov, A. G., and Azizullayev, M. G. (2024). Analysis of modules and systems used in effective control of UAVs in radio electronic combat environment. *Impress*, 47-48. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/389079f8-888a-4f84-bdda-84c954cea0f1/content
16. Sinha, D., Verma, A. və Kumar, S. (2016). Software defined radio: Operation, challenges and possible solutions. *2016 International Conference on Information Systems and Computer Networks (ISCON)*, 1–5. https://doi.org/10.1109/ISCO.2016.7727079

Received: 26.11.2024
Accepted: 01.03.2025