https://doi.org/10.70265/FKJC9739

INTERVENTION METHODS IN CONTROL AND COMMUNICATION SYSTEMS OF UNMANNED AERIAL VEHICLES, ANALYSIS AND EVALUATION OF SIGNAL QUALITY

Fakhreddin Aghayev, Asad Rustamov, Mehman Binnatov, Mukhtar Azizullayev, Aliagha Sahibcanov

Summary: *This research investigates the methods of radio-electronic warfare (REW) against the control and communication systems of unmanned aerial vehicles (UAVs) and analyzes the performance of their telemetry systems. The growing use of UAVs in both military and civilian applications makes it essential to prevent REW interventions targeting their communication and control systems.*

The study analyzes the effects of GPS jamming, spoofing, electromagnetic pulses (EMP), cyberattacks, and artificial intelligence-based interference technologies on UAVs. REW interventions are used to disrupt UAV communication, cause loss of control, or render them functionally inoperative. In particular, blocking or falsifying GNSS signals can cause UAVs to operate with incorrect coordinates or completely lose control.

The distance-dependent changes in communication parameters such as Path Loss (PL) and Signal-to-Noise Ratio (SNR) in UAV communication systems were modeled using the Python programming language. Graphs showing the relationship between distance and Path Loss, and distance and SNR were generated using the Matplotlib library.

The diagrams indicate that high-frequency modules (XBee PRO S2C – 2.4 GHz) experience greater Path Loss and a faster decline in communication quality. In contrast, low-frequency modules (RFD900+ – 900 MHz and TBS Crossfire – 868 MHz) provide more stable communication and allow signals to propagate over longer distances.

The findings of this study show that enhancing the resilience of UAVs to REW attacks requires the use of low-frequency communication modules, implementation of anti-jamming technologies, and development of defense strategies such as adaptive frequency hopping. This research provides a scientific foundation for improving the effectiveness of UAV control and communication systems against REW interference.

Keywords: *UAV, GPS, GNSS, REW, Autonomous flight mode, Electromagnetic pulse, Signal jamming, Anti-jamming technologies, Telemetry, Path Loss, Python, Matplotlib*

INTRODUCTION

In recent years, various types of unmanned aerial vehicles (UAVs) have been increasingly utilized on the battlefield and in operations, transforming from a rarely used and limited weapon system into a widely deployed instrument of armed conflict. Over time, the course and outcome of military operations, the combat readiness of armed forces, and their ability to accomplish assigned missions have begun to significantly depend on the degree and scale of UAV deployment (Rüstəmov, Azizullayev, & Şəzəli, 2023). UAVs have become a powerful supporting tool for commanders in making decisions about the initiation of combat operations. They are continuously evolving and improving, and are widely used in modern warfare both as reconnaissance and strike assets. These developments necessitate a thorough and comprehensive analysis of all aspects of UAV application.

An analysis of the development directions of combat forms and methods shows that unmanned aviation is now regarded as a highly effective means capable of carrying out a wide range of combat missions (Rüstəmov, Məmmədzadə, Məlikov, Həşimov, & Azizullayev, 2024). For UAVs to operate effectively, the stable functioning of their control and communication systems is essential. These systems allow UAVs to regulate their flight trajectory and be operated remotely via space-based radio navigation systems (GPS, GLONASS, Galileo, BeiDou), telemetry channels, and command-control links.

However, the use of radio-electronic warfare (REW) tools can significantly impact UAV control systems and communication channels, potentially limiting or completely disrupting their operational capabilities. In particular, GNSS signal jamming, GPS spoofing, high-energy electromagnetic pulses (EMP), and artificial intelligence-based automated interference technologies are methods developed to effectively disrupt UAV control and communication systems (Rüstəmov, Məmmədzadə, Məlikov, Həşimov, & Azizullayev, 2024; Rustamov, Gasanov, & Azizullayev, 2024a; Куприянов, Шустов, 2011).

This scientific research investigates the methods of interference in UAV control systems and communication channels, the mechanisms of these methods, and the risks they pose to UAV operation. Additionally, the role of satellite-based radio navigation systems (GPS, GLONASS, Galileo, BeiDou) in UAV control and their disruption through REW technologies will be analyzed in detail.

The main objective of the study is to develop effective REW methods against UAVs, assess the potential impact of these technologies, and propose strategic solutions for developing more resilient control and communication systems in the future.

EXPOSITION

Global Navigation Satellite Systems (GNSS) are critically important for the precise positioning, orientation, and autonomous control of unmanned aerial vehicles (UAVs) (Rüstəmov, Azizullayev, & Şəzəli, 2023). Through systems such as GPS, GLONASS, Galileo, and BeiDou, UAVs determine their flight trajectory in real time, move toward their target, and are controlled by an operator. Without these systems, the autonomous operation of UAVs becomes limited, and their overall effectiveness is significantly reduced (Rustamov, Gasanov, Azizullayev, 2024c; Genç, & Erciyes, 2020).

UAVs receive GNSS signals to accurately determine their position and construct optimal flight paths based on this data. The information obtained from GPS, GLONASS, and other navigation systems ensures stable and reliable flight, regardless of weather conditions. In autonomous flight mode, GNSS coordinates allow UAVs to follow pre-programmed routes. Additionally, automatic take-off and landing systems are managed based on GPS coordinates, and UAVs continuously adjust their trajectory using GNSS data to enhance flight safety.

The use of GNSS in both military and civilian UAV missions holds great importance. In reconnaissance and surveillance operations, GNSS enables the accurate determination of object coordinates. On the battlefield, military UAVs use GPS coordinates to detect and destroy targets. Furthermore, UAV control and telemetry systems utilize GPS for time synchronization. Two or more UAVs participating in a mission can coordinate and operate synchronously based on GNSS data (Kaplan, & Hegarty, 2017).

Table 1. Technical Specifications of the GPS (Global Positioning System)

No.	Specification	Information
1	Country of Origin	USA
2	Controlling Authority	U.S. Department of Defense (DoD)
3	Orbital Altitude	20,200 km
4	Orbital Planes	6
5	Number of Satellites	31
6	Frequencies	L1: 1575.42 MHz, L2: 1227.60 MHz, L5: 1176.45 MHz
7	Accuracy	Civilian: ±5 m, Military: ±30 cm
8	Initial Operation Date	1978 (test), 1995 (fully operational)
9	Orbital Period	~12 hours

Advantages of the GPS System:

1. It is the most widely used GNSS system in the world.
2. It can provide military-grade accuracy up to 30 cm.
3. It is compatible with numerous civilian and military applications.

Disadvantages of the GPS System:

1. GPS signals can be vulnerable to military interference (jamming, spoofing).

2. It is controlled by the United States, and signal restriction is possible in certain cases.

Table 2. Technical Specifications of the GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema) System

No.	Specification	Information
1	Country of Origin	Russia
2	Controlling Authority	Roscosmos
3	Orbital Altitude	19,100 km
4	Orbital Planes	3
5	Number of Satellites	24
6	Frequencies	L1: 1602 MHz, L2: 1246 MHz, L3: 1202 MHz
7	Accuracy	Civilian: ±5–7 m, Military: ±20 cm
8	Initial Operation Date	1982 (test), 1996 (fully operational)
9	Orbital Period	~11 hours 15 minutes

Advantages of the GLONASS System:

1. Performs better at high latitudes (near the poles).

2. Accuracy improves when used in combination with GPS.

Disadvantages of the GLONASS System:

1. Its accuracy is slightly lower compared to GPS and Galileo.

2. Due to the lower number of satellites, signal coverage may be weak in some regions.

Table 3. Technical Specifications of the Galileo System

No.	Specification	Information
1	Country of Origin	European Union
2	Controlling Authority	ESA (European Space Agency)
3	Orbital Altitude	23,222 km
4	Orbital Planes	3
5	Number of Satellites	30 (24 active + 6 spare)
6	Frequencies	E1: 1575.42 MHz, E5: 1191.795 MHz, E6: 1278.75 MHz
7	Accuracy	Civilian: ±1 m, Military: ±20 cm
8	Initial Operation Date	2011 (test), 2020 (fully operational)
9	Orbital Period	~14 hours

Advantages of the Galileo System:

1. Provides higher accuracy for civilian use (below 1 meter).

2. Accuracy increases when used in combination with GPS and GLONASS.

3. Its operation is fully controlled by Europe and is not subject to restrictions by the US or Russia.

Disadvantages of the Galileo System:

1. Not yet fully widespread and has limited compatibility with some devices.

Table 4. Technical Specifications of the BeiDou (BDS – BeiDou Navigation Satellite System)

No.	Specification	Information
1	Country of Origin	China
2	Controlling Authority	People's Republic of China (CNSA)
3	Orbital Altitude	MEO: 21,500 km, GEO: 35,786 km, IGSO: 19,100 km
4	Orbital Planes	3 (MEO, GEO, IGSO)
5	Number of Satellites	35
6	Frequencies	B1: 1575.42 MHz, B2: 1207.14 MHz, B3: 1268.52 MHz
7	Accuracy	Civilian: ±5 m, Military: ±10 cm
8	Initial Operation Date	2000 (test), 2020 (fully operational)
9	Orbital Period	~12 hours

Advantages of the BeiDou System:

1. Provides stronger signals and higher accuracy for Asia and Africa.

2. Offers increased accuracy when used together with GPS and Galileo.

3. Managed by China, making it a viable alternative as an independent system.

Disadvantages of the BeiDou System:

1. Its global coverage is not as extensive as GPS and Galileo.

2. It is not yet fully optimized for some international civilian UAVs.

1. Optimal Navigation Choice for Unmanned Aerial Vehicles (UAVs)

The optimal GNSS system for UAVs depends on their intended purpose (Макаренко, 2020).

• **For military and security purposes:** GPS + Galileo + GLONASS (multisystem support provides greater resistance to signal interference).

• **For civilian and commercial use:** Galileo + GPS (offers higher accuracy for civilian applications).

• **For UAVs operating in the Asian region:** BeiDou + GPS + Galileo (stronger signal coverage over Asia and Africa).

• **For Arctic and polar regions:** GLONASS + GPS (GLONASS performs better at high latitudes).

The combined use of GPS, Galileo, and GLONASS systems is the most optimal option to ensure stable, accurate, and secure UAV operations. This combination is more resilient to signal disruptions and provides high accuracy. For military applications, Galileo and BeiDou can also be used as alternatives alongside GPS. By utilizing global navigation satellite systems (GNSS), unmanned aerial vehicles (UAVs) gain the following capabilities (Макаренко, 2020; Куприянов, Шустов, 2011):

• **Autonomous Navigation:** UAVs can navigate autonomously using GPS and other radionavigation systems.

• **Accurate Positioning:** Military and civilian UAVs use GNSS systems to precisely identify targets and accomplish missions.

• **Real-Time Coordination:** Remotely controlled or AI-powered UAVs can determine and adjust their trajectories in real time.

1.1 Methods of Interference with UAV Control Systems and Communication Channels

Interfering with the control and communication systems of unmanned aerial vehicles (UAVs) is one of the main tactics in modern electronic warfare (EW). These interventions are primarily carried out to limit the operational capabilities of enemy UAVs, disable their control, or redirect them in the wrong direction (Rustamov, Gasanov, & Azizullayev, 2024b; Rustamov, Gasanov, Azizullayev, 2024c).

The methods of interfering with UAV communication and control systems can generally be divided into three (3) main categories:

- Signal Jamming: This technique disrupts the UAV's control and communication signals, rendering the drone functionally inoperable.

- GPS Jamming – By blocking GNSS signals (GPS, GLONASS, Galileo, BeiDou), it is possible to disrupt the UAV's accurate positioning. This method typically involves the transmission of high-power interference signals.

- Communication Jamming – This involves jamming control signals to sever the UAV's connection with the operator. Communication channels operating in the 2.4 GHz and 5.8 GHz frequency bands are particularly targeted.

- Telemetry Jamming – This method interferes with the telemetry channels of UAVs to obstruct the transmission of data. It can significantly weaken real-time communication between the UAV and the operator.

1.2 Signal Spoofing

Signal spoofing is a technique in which false information is sent to a UAV's control systems to mislead it into changing direction or to hijack its control.

-GPS Spoofing – Fake signals are transmitted to the UAV's GPS receiver, causing it to believe it is in a different location. This may lead the UAV to change its course or enter a secure zone controlled by the adversary.

-Communication Spoofing – The UAV's communication signals are intercepted and replaced with newly generated control signals by the adversary. This method can be used to hijack the UAV and reprogram it.

1.3 Physical and Cyber Attacks

Physical and cyber intervention methods are also widely used against UAV control and communication systems.

- **Cyberattacks** – UAVs with unencrypted or weakly protected control protocols can be hacked, allowing attackers to seize control.
- **Electromagnetic Pulse (EMP) Attacks** – High-powered electromagnetic pulses can disable the electronic systems of UAVs.
- **Laser and High-Power Microwave Weapons** – These can physically damage the UAV's sensors and communication modules, rendering the UAV non-functional.

1.4 Countermeasures and Defense Techniques

Several countermeasures exist to protect UAV control systems and communication channels from interference.

- **Anti-Jamming Technologies** – Advanced signal filtering and multi-channel reception systems increase UAV resilience to jamming.
- **Encrypted Communication** – Secure communication can be ensured using strong encryption protocols such as AES and RSA.
- **Autonomous Flight Systems** – UAVs can continue their missions along pre-programmed trajectories even after losing GNSS and communication signals.
- **Adaptive Frequency Hopping** – UAVs can operate across different frequency bands to resist jamming and spoofing attempts.

2. Path Loss and SNR: Their Relationship and Importance in Communication Systems

To ensure the efficient operation of communication systems, it is essential to calculate and analyze two key parameters: Path Loss (PL) and Signal-to-Noise Ratio (SNR). Path Loss describes the reduction in signal power as it travels from the transmitter to the receiver, while SNR indicates the ratio of signal power to noise power. The higher the SNR, the cleaner the signal with less noise. These two parameters are closely related and together influence signal quality (Mahmood, Gidlund, & Åkerberg, 2019; Hassan, Khan, & Rehman, 2020).

SNR Formula:

The Signal-to-Noise Ratio (SNR) is generally expressed as the ratio of signal power to noise power as follows (Mahmood, Gidlund, & Åkerberg, 2019):

$$\boldsymbol{SNR = \frac{Ps}{Pn}} \tag{1}$$

Where:

Ps – Signal power (in watts or milliwatts)

Pn – Noise power (in watts or milliwatts)

The more commonly used and practically analyzed form of SNR is expressed in decibels (dB) and is given by the following formula (2) (Mahmood, Gidlund, & Åkerberg, 2019):

$$\boldsymbol{SNR_{dB} = 10log_{10}(\frac{Ps}{Pn})} \tag{2}$$

2.1. Path Loss: Path Loss refers to the reduction in the power of electromagnetic waves as they propagate from the source to the receiver. This loss mainly occurs due to atmospheric conditions, distance, and the presence of obstacles.

2.2. Free Space Path Loss (FSPL): Free Space Path Loss describes the signal attenuation when it propagates through free space without any obstacles. It is calculated using the Friis transmission equation and is expressed as follows (Mahmood, Gidlund, & Åkerberg, 2019):

$$\boldsymbol{PL = (\frac{4\pi df}{c})^2} \tag{3}$$

(Mahmood, Gidlund, & Åkerberg, 2019)

Or it can also be expressed in decibels (dB) as in equation (4):

$$\boldsymbol{PL_{dB} = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}(\frac{4\pi}{c})} \tag{4}$$

(Mahmood, Gidlund, & Åkerberg, 2019)

Where:

PL – Path Loss (in dB)

d – Distance (in meters)

f – Frequency (in Hz)

c – Speed of light (3×10^8 m/s)

If the distance is given in kilometers (km) and the frequency in megahertz (MHz), the simplified formula can be expressed as in equation (5) (Mahmood, Gidlund, & Åkerberg, 2019).

$$\boldsymbol{PL_{dB} = 32.44 + 20log_{10}(d) + 20log_{10}(f)} \tag{5}$$

(Mahmood, Gidlund, & Åkerberg, 2019)

Where:

d – Distance (in kilometers)

f – Frequency (in megahertz)

32.44 – A constant value that accounts for signal propagation in free space.

2.3. Path Loss (PL) and Its Impact on SNR

Path Loss (PL) refers to the weakening of an electromagnetic signal during transmission due to various factors. These factors include:

- Signal propagation through free space

- Atmospheric effects (rain, fog, humidity, etc.)

- Infrastructure obstacles (buildings, trees, etc.)

- Reflections and fading from the Earth's surface

Path Loss causes a reduction in the signal power by the time it reaches the receiver. The power received by the antenna can be expressed using the PT formula (6) as follows (Mahmood, Gidlund, & Åkerberg, 2019):

$$\boldsymbol{P_r = P_t - \mathrm{PL}} \tag{6}$$

Where:

Pr – Received signal power at the antenna (in dBm or dBW)

Pt – Transmitted signal power from the antenna (in dBm or dBW)

PL – Power lost during transmission (in dB)

Signal attenuation at the receiving antenna affects the SNR, because as the received signal power **Pr** decreases, the SNR also decreases.

1. The Relationship Between SNR (Signal-to-Noise Ratio) and Path Loss:

SNR represents the ratio of the signal power to the noise level at the receiving antenna and is calculated using the following formula (7) (Mahmood, Gidlund, & Åkerberg, 2019):

$$\boldsymbol{SNR_{Db} = P_t - P_n} \tag{7}$$

Where:

Pn – Noise power (in dBm or dBW)

Pr – Received signal power at the antenna

As Path Loss increases, Pr decreases, and consequently, SNR also decreases. In other words, as the signal power weakens relative to the noise, the performance of the communication system degrades (Mahmood, Gidlund, & Åkerberg, 2019). The Bit Error Rate (BER), which is related to SNR, also increases – meaning that the signal error rate rises and the communication quality deteriorates.

2.4. The Impact of Path Loss and SNR on Communication Systems

Table 5. The role of Path Loss and SNR in communication systems

No.	System	Path Loss	SNR	Result
1	Mobile communication (4G, 5G)	High over long distances	Low	Communication quality decreases, transmission errors increase
2	Wi-Fi networks	Affected by walls in indoor environments	May decrease	Signal weakening reduces internet speed
3	Satellite communication	Very high over long distances	May be low	Signal weakening leads to degraded communication quality
4	Radar systems	Influenced by atmospheric and environmental factors	Must be high	Strong signals are required for detecting enemy targets

In addition, in military communication systems, electronic warfare devices (jammers) create artificial noise, lowering the SNR and disrupting communication.

2. Mathematical Modeling of Telemetry Modules in UAVs, and Calculations of Path Loss and SNR

The Path Loss and SNR values presented in the tables were calculated based on Equation (1) and Equation (2). Path Loss values were computed using the Friis transmission equation according to the free space propagation model (Equation 1). Signal-to-Noise Ratio (SNR) values were calculated based on the transmitted signal power, noise power, and Path Loss using Equation (2).

Using these formulas, Path Loss and SNR values varying with distance were calculated for the following telemetry modules: XBee PRO S2C (2.4

GHz), RFD900+ (900 MHz), and TBS Crossfire (868 MHz) (see Table 6, Table 7, Table 8).

Table 6. Path Loss and SNR Calculations for the XBee PRO S2C (2.4 GHz) Telemetry Module

S/S	Distance (m)	Path Loss (dB)	SNR (dB)
1.	100	80.05	37.95
2.	200	86.07	31.93
3.	300	89.60	28.40
4.	400	**92.10**	25.90
5.	500	94.03	23.97

Table 7. RFD900+ (900 MHz) path loss and SNR calculations for the telemetry module

S/S	Distance (m)	Path Loss (dB)	SNR (dB)
1.	100	71.22	46.78
2.	200	77.24	40.76
3.	300	80.76	37.24
4.	400	83.26	34.74
5.	500	85.20	32.80

Table 8. TBS Crossfire (868 MHz) path loss and SNR calculations for the telemetry module

S/S	Distance (m)	Path Loss (dB)	SNR (dB)
1.	100	71.22	46.78
2.	200	77.24	40.76
3.	300	80.76	37.24
4.	400	83.26	34.74
5.	500	85.20	32.80

3. Visualization of Distance-Dependent Changes in Path Loss and SNR in UAVs Using Python

The distance-dependent variation of Path Loss and SNR is illustrated in the graphs below. These graphs represent real calculations obtained for the telemetry modules XBee PRO S2C (2.4 GHz), RFD900+ (900 MHz), and TBS Crossfire (868 MHz). The results show that as the distance increases, Path Loss also increases, while SNR decreases. Modules operating at lower frequencies (RFD900+ and TBS Crossfire) are able to maintain signal quality over longer distances.

Figure 1 shows the graph of the relationship between distance and Path Loss based on Equation (3).

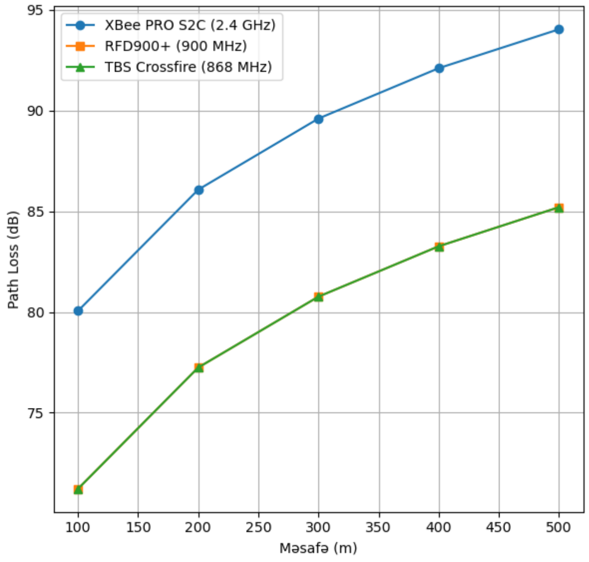

Figure 1. The relationship between distance and Path Loss

The graph shows that as the distance increases, Path Loss (signal attenuation) also increases. The XBee PRO S2C (2.4 GHz) module, which operates at a higher frequency, experiences greater Path Loss, indicating that signal strength decreases more rapidly over long distances. In contrast, the RFD900+ (900 MHz) and TBS Crossfire (868 MHz) modules exhibit lower Path Loss, thus providing more stable communication over longer distances. This result confirms that lower frequencies are more effective for long-range communication.

Figure 2 illustrates the variation of SNR with distance, calculated using the (1) SNR formula and the (2) Path Loss formula.

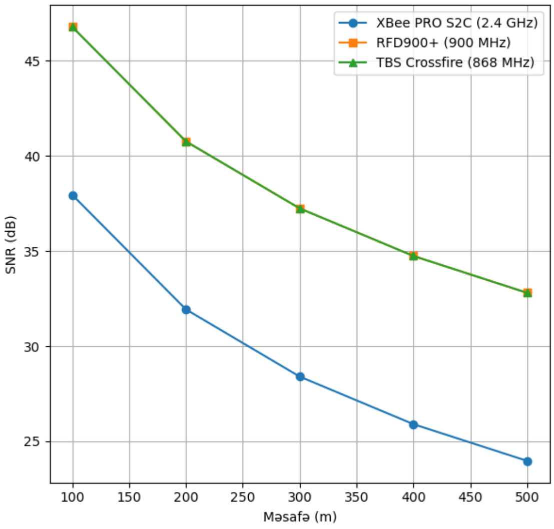

Figure 2. The relationship between distance and SNR

The graph shows that as the distance increases, the SNR (Signal-to-Noise Ratio) decreases. The main reason for this is that as the signal moves further away from the transmitter, it becomes weaker, and environmental noise has a greater impact on the signal strength. The high-frequency XBee PRO S2C (2.4 GHz) module experiences higher Path Loss, resulting in a faster decline in SNR values. In contrast, the lower-frequency RFD900+ (900 MHz) and TBS Crossfire (868 MHz) modules provide more stable communication and maintain higher SNR values. This result indicates that low-frequency modules are more suitable for long-range and reliable communication in UAVs.

CONCLUSION

This research examined the impact of radio-electronic warfare (REW) interference on the control and communication systems of unmanned aerial vehicles (UAVs), as well as strategies that can be implemented to enhance resilience against such interference. The widespread military and civilian applications of UAVs make it critical to prevent attacks on their control and communication systems.

Within the scope of the study, GPS jamming, spoofing, electromagnetic pulse (EMP), cyberattacks, and artificial intelligence-based interference technologies were analyzed, and their effects on UAV control and communication were investigated. The main outcomes of these interferences include loss of control, navigation based on false coordinates, and disrupted communication.

The distance-dependent changes in Path Loss (PL) and Signal-to-Noise Ratio (SNR) in UAV communication systems were modeled using the Python programming language. The calculations showed that high-frequency telemetry modules (XBee PRO S2C – 2.4 GHz) are more susceptible to Path Loss, leading to a rapid decline in communication quality. In contrast, lower-frequency modules (RFD900+ – 900 MHz and TBS Crossfire – 868 MHz) maintain better signal quality and more stable communication over long distances.

The study's results indicate the necessity of implementing several technological solutions to enhance UAV communication system resilience against REW attacks. First, interference signals can be blocked using anti-jamming technologies, and jamming attempts can be detected through spectral analysis techniques. Additionally, secure communication protocols, particularly strong encryption methods such as symmetric encryption algorithms (AES) and asymmetric encryption algorithms (RSA), play a vital role in protecting control and telemetry channels from cyberattacks.

To improve the resilience of communication systems against interference, the application of adaptive frequency hopping technology is also crucial. This technology allows UAVs to operate across multiple frequency bands, making communication more flexible and resistant to interference. At the same time, it is advisable to avoid sole reliance on GPS by integrating alternative GNSS technologies. The incorporation of satellite navigation systems such as Galileo, GLONASS, and BeiDou, along with autonomous navigation solutions like IMU (Inertial Measurement Unit), enhances the stability of UAV control and navigation systems and makes them more robust against REW attacks.

The combined use of these technologies increases UAV resistance to interference and ensures reliable operation.

In conclusion, this study provides a scientific foundation for developing new strategies to more effectively defend UAV control and communication systems against REW attacks. The results show that the use of low-frequency communication modules and the implementation of advanced defense technologies are essential for maintaining long-term and stable communication links in UAVs. Future research should focus on testing these defense strategies and developing new solutions to achieve higher levels of effectiveness.

BIBLIOGRAPHY:

Куприянов, А. И., Шустов, Л. Н. (2011). *Радиоэлектронная борьба. Основы теории*. Москва: Вузовская книга. ISBN 978-5-9502-0444-9. // Kupriyanov, A. I., Shustov, L. N. (2011). Electronic Warfare. Fundamentals of Theory. Moscow: Vuzovskaya Kniga (in Russian). ISBN 978-5-9502-0444-9.

Макаренко, С. И. (2020). Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 4. Функциональное поражение сверхвысокочастотными и лазерным излучением. *Системы управления, связи и безопасности*, (3), 122-157. DOI: 10.24411/2410-9916-2020-10304. // Makarenko, S. I. (2020). Counter Unmanned Aerial Vehicles. Part 4. Functional Destroying with Microwave and Laser Weapons. *Systems of Control, Communication and Security*, (3), 122-157 (in Russian). DOI: 10.24411/2410-9916-2020-10304.

Genç, Y., & Erciyes, E. (2020). İnsansız Hava Araçları (İHA) Tehditleri ve Güvenlik Yönetimi. *Türkiye İnsansız Hava Araçları Dergisi, 2*(2), 36-42. https://dergipark.org.tr/tr/download/article-file/1250495

Hassan, K., Khan, R., & Rehman, S. (2020). *Impact of Jamming and Spoofing on UAV Communication Systems: A Survey*. IEEE Access.

Kaplan, E. D., & Hegarty, C. (2017). *Understanding GPS/GNSS: Principles and Applications* (3rd ed.). Artech House. https://vuxuandinh.com/Tailieu/GPS/2017-Understanding%20GPSGNSS%20by%20Hegarty,%20Christopher%20Kaplan,%20Elliott%20D%20(z-lib.org).pdf

Mahmood, A., Gidlund, M., & Åkerberg, J. (2019). *Reliable Wireless Communications for Industrial IoT: Performance Evaluation and Channel Modeling*. IEEE Transactions on Wireless Communications.

Rustamov, A. R., Azizullayev, M. Q., & Shazali, E. (2023, November 1-2). Features of conducting radio and radio technical reconnaissance in mountainous conditions and in the lowland zone. *Republican scientific and practical conference on the 100th anniversary of the birth of Heydar Aliyev and modern military art in global security* (pp. 509-511).

Rustamov, A. R., Gasanov, A. G., & Azizullayev, M. G. (2024a). Analysis of modules and systems used in effective control of UAVs in radio electronic combat environment. *14th international conference science and technology Conf., 25-26 April 2024, Baku–Kharkiv–Zhilina* (pp. 47-48). Kharkiv: Impress. https://repository.kpi.kharkov.ua/handle/KhPI-Press/77137

Rustamov, A. R., Gasanov, A. G., & Azizullayev, M. G. (2024b). The role of navigational and hydrographical support in ensuring security of the Caspian Sea. *2nd International Conference on Logistics, Transport and Distribution in the Caspian Region, May 15-17, Baku, Azerbaijan*.

Rustamov, A. R., Gasanov, A.G., Azizullayev, M.G. (2024c). Effective Application of Telemetry Systems in Unmanned Aerial Vehicles. In *Current Directions of Development of Information and Communication Technologies and Control Tools, Proceedings of 14-th International Scientific and Technical Conference April 25 – 26, 2024*, Volume 2: sections 3, 4, 5, 6 (pp. 69-70). https://doi.org/10.32620/ICT.24.t2 // *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління, Тези доповідей чотирнадцятої міжнародної науково-технічної конференції 25 – 26 квітня 2024 року,* Том 2: секції 3, 4, 5, 6 (стр. 69-70). https://doi.org/10.32620/ICT.24.t2

Rüstəmov, Ə. R., Məmmədzadə, F., Məlikov, F., Həşimov, R., & Azizullayev, M. (2024). Xəzər dənizində təhlükəsizliyin təmінində naviqasiya və hidroqrafiya təminatının rolu. *Azərbaycan Respublikası Müdafiə Nazirliyi Milli Müdafiə Universiteti Hərbi bilik elmi-nəzəri jurnalı*, (2), 65-75. // Rustamov, A. R., Mammadzadeh, F., Malikov, F., Hashimov, R., & Azizullayev, M. (2024). The role of navigation and hydrographic support in ensuring security in the Caspian Sea. *National Defense University of the Ministry of Defense of the Republic of Azerbaijan Scientific and Theoretical Journal of Military Knowledge*, (2), 65-75.