Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 127 **2025**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2025.127.9

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Mammadov, A., Sadigov, G. Implementation of complex solutions for protection against cyber threats of electronic systems of unmanned aerial vehicles. *Scientific Journal of Silesian University of Technology. Series Transport*. 2025, **127**, 155-164. ISSN: 0209-3324. DOI: https://doi.org/10.20858/sjsutst.2025.127.9

Aftandil MAMMADOV[1], Gurban SADİGOV[2]

IMPLEMENTATION OF COMPLEX SOLUTIONS FOR PROTECTION AGAINST CYBER THREATS OF ELECTRONIC SYSTEMS OF UNMANNED AERIAL VEHICLES

Summary. In the article, the possibilities of applying complex solutions to protect the electronic systems of unmanned aerial vehicles (UAVs) and other important processes from cyber threats were considered. The current application of UAVs in various fields makes the security of their electronic systems relevant. Aerial vehicles can be subject to attacks by attackers who exploit physical, network, and software vulnerabilities in the data exchange process. The article analyzes such methods as data encryption, encoding methods, publishing fake data, and protection against Global Positioning System spoofing attacks. The proposed complex approaches are integrated into the existing systems of UAVs, allowing to increase the level of their security. Complex solutions involve the integration of a special encryption and coding block, as well as the implementation of a module for comparing coordinates and broadcasting false signals.

Keywords: unmanned aerial vehicles, electronic systems, cyber-attacks, encoding and encryption, GPS spoofing, sensor, inertial navigation system, communication system

[1] Department of Avionics, Faculty of Air Transport, National Aviation Academy, Baku, Azerbaijan, Mardakan ava.30. Email: aftandilmammadov@naa.edu.az. ORCID: https://orcid.org/0000-0003-0842-4230
[2] Department of Avionics, Faculty of Air Transport, National Aviation Academy, Baku, Azerbaijan, Mardakan ava.30. Email: gsadigov@naa.edu.az. ORCID: https://orcid.org/0009-0006-8730-7452

1. INTRODUCTION

UAVs, which in the early days were used only for military and observation purposes, have also begun to be applied in engineering, scientific research and civilian areas due to the reduction in costs and increased accessibility with the technology that has developed in recent years [1]. UAVs use various active or passive sensors to obtain the necessary information from these areas with high accuracy. UAVs with these capabilities are capable of providing more accurate, sensitive, fast information and analytical solutions than manned flight equipment or satellite imagery.

While UAVs provide professionals with numerous opportunities in the military, commercial, and civilian fields, their management and information exchange face serious cyber threats. These threats can allow criminal attackers to easily perform attacks against systems. Therefore, it is very important to strengthen information exchange channels, apply encryption and encoding methods.

This ensures widespread use in natural disaster monitoring, military operations, agriculture, and logistics. UAVs are engaged in the collection and transmission of sensitive information (for example, intelligence, military, or strategic information). If this information is intercepted by the enemy, serious security risks may arise [2].

In recent years, UAVs, especially those used during wartime, have been exposed to numerous cyber threats. In addition, since UAVs operate alone rather than in a group form, it becomes conveniently possible to apply outside effects to them.

2. LITERATURE REVIEW

Every year, the types of cyberattacks and the possibility of threats against UAVs are increasing. This is due to the fact that they become more functional depending on the requirements that are pursued against them. Currently, as SDR (Software Definition Radio) is widespread, the number of possible attack channels is multiplying. As examples of cyber-attacks against UAVs, the following can be highlighted:

- GPS spoofing;
- Interception of communication channels;
- Malware attacks;
- Denial-of-Service (DoS) attacks;
- Using Firmware vulnerabilities;
- Man-in-the-Middle (MitM) attack;
- Theft of camera and sensor data;
- Fake UAV attacks (Clone Attack).

Many of these attacks took place in real, and some were executed for testing.

In GPS spoofing attacks, an attacker manipulates the UAV's location information by transmitting fake GPS signals to it. This can cause the drone to be misdirected or deviated from the designated area. An example of such interference can be seen in the 2011 incident, when Iran claimed that the United States had launched an RQ-170 Sentinel unmanned aerial vehicle by spoofing GPS signals. Iran manipulated the UAV with fake GPS signals and landed it in what it identified as a friendly area [8].

The communication channel between the UAV and the control center is vulnerable to cyberattacks. By capturing this channel, attackers can change the control of the UAV or steal sensitive information. During the analysis of DJI drones in 2018, it was determined that communication could be intercepted due to poor encryption of control signals [6].

By embedding malware in the software or operating system of the UAV, its normal operation can be disrupted. An attacker can disable the drone's sensors, cameras, or other components through malware. In 2019, researchers in this field, were able to exploit vulnerabilities in some UAV models to install malware on the system and take full control of the drone [11, 12].

Cameras and sensors on UAVs collect highly sensitive information. Attackers can steal this information in real time and use it for their own purposes. In 2020, some security researchers took advantage of the fact that drones are not encrypted during the transmission of video data, proving that this information can be easily stolen [9].

An attacker can create a fake UAV (clone) and present it as a real drone, or manipulate the exchange of information by moving to the location of the real drone. For example, during hostilities, the attackers ensured the misdirection of intelligence information by using fake UAVs that looked like real UAVs [7].

It should be noted that more avionics systems are threatened during cyberattacks on UAVs. Here, in particular, we can highlight the communication and navigation systems.

3. ISSUE SOLVING AND DISCUSSION

It is quite important to have a complex approach to ensure the complete safety of UAVs. The proposed comprehensive approach includes two main methods:

1. The first of these approaches is the use of special encryption, encoding, and authentication equipment at any stage of the information exchange process and in the case of transmission through any channel. This approach can allow preserving the confidentiality and integrity of information. To accomplish this task, an encoding and encryption module must be added to the standard structural scheme. As a central unit, the module will control the exchange of information over all channels. Of course, it is impossible to fully achieve a solution to the issue with the integration of this module alone. In order to achieve the desired result, it is important to improve the modules mentioned in the following parts of .
2. If we look at the second approach, it is intended to create and broadcast false signals in order to distract the effects that are a threat. In order to strengthen security, it is possible to create fake access points that the other party can detect and allow keeping the real data transmission confidential. Many models of UAVs are known as Wi-Fi access points and allow operators to control them by connecting. In the proposed new approach, our module creates several access points that correspond to real UAV parameters in different frequency bands or different channels, depending on their purpose.

For the complex application of both of the above approach, a structural scheme was developed using the SysML system modelling language (Fig. 1).

During the construction of this scheme, it is planned to implement a complex method with the integration of as few blocks as possible. In order for UAVs to perform the tasks, it is necessary to focus on mass issues.

3.1. Determination of element base

The application of special modules is necessary for the implementation of this complex approach. Taking into account that the UAVs currently in use are exchanged for more and more information, the elements selected must also meet modern requirements. Of great importance are the image images taken by UAVs or the video data they reflect in real time. It is important to take into account such moments and introduce special processors and other devices. But on the other hand, it is necessary to pay attention to weight and dimensions so that the UAV does not lose its agility. Taking into account the stated, the analysis and selection of modules presented in the structural scheme were carried out.

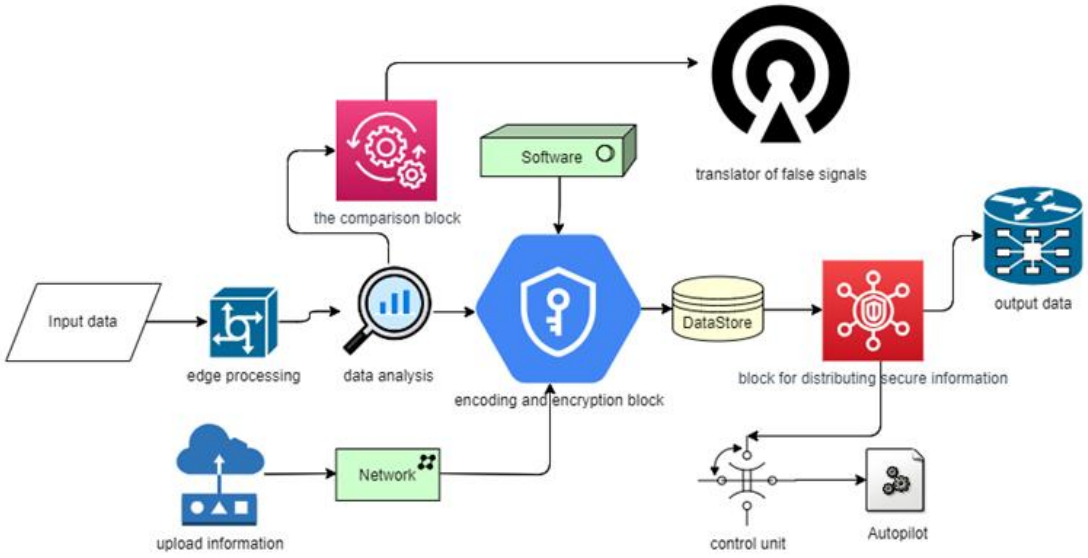

Fig. 1. Structural scheme of an integrated approach to ensuring the safety of UAVs

When selecting components, it is essential to consider their compatibility and potential for integration with the existing systems used on UAVs.

3.1.1. Data processing module

The data processing module (edge processing) executes many operations. At its core, this module provides data collection. It involves receiving information from sensors, cameras, GPS receivers, and other sources. Then the process of preparing the data for transmission is provided. Here, UART, I2C, SPI interfaces can be used to connect sensors. Interfaces that can be saved do not have built-in authentication or encryption mechanisms. These interfaces do not guarantee that the data comes from the right device. During their use, the risk of signal interception or interference from outside devices increases. However, currently mentioned interfaces are considered to be suitable for ensuring the security of coding and encryption block reflected in the structural scheme.

Information enters this module from the receiver. The data processing module consists of a controller and a processor. Depending on the specific purpose of the UAV, different controllers may be used.

The authors examined the Pixhawk, CubePilot and MicroPilot MP2128 controllers with high tactical and technical characteristics. Pixhawk controller supports Px4 and ArduPilot. The CubePilot controller is a high-performance controller with reservation. The MicroPilot MP2128 is a certified controller for professional and military applications [3].

3.1.2. Data analysis module

The data analysis module is designed for processing large amounts of data coming from UAV sensors and communication systems. This module plays a key role in ensuring the autonomy and efficiency of the hardware, including increasing resistance to cyber threats. The mentioned module analyzes the information received using the algorithms on the device in real-time cross-section.

Data analysis allows the identification of cyber-attacks, including attempts to seize control, interfere with data transmission, or apply malicious software. Here it is necessary to pay attention to the high productivity and the choice of elements for performing complex calculations. Given the rapid development of technology in the near future, NVIDIA Jetson or Intel Movidius processors will be suitable for the mentioned operations. After eliminating noise and unnecessary information in the data analysis algorithms, clustering should be carried out. In the process of clustering, data is divided into groups to facilitate analysis. For specific tasks, object recognition and prediction can be applied based on trained models.

Since the reconciliation of elements selected by electronics systems is an important issue, this point is taken into account when selecting parts of the data analysis module and other element base. The data analysis module is an important part of modern UAVs, ensuring their reliable and safe operation even in difficult conditions. The module transmits information in two directions. One of them is the encoding and encryption block and the other is the comparison module.

3.1.3. Encoding and encryption block

Encoding and encryption block for Unmanned Aerial Vehicles is a critical component for ensuring security, increasing data protection and resistance to intrusion. This block is used both for communication and for data protection in the flight system.

Various encryption technologies can be applied for UAVs with the proposed block tool. If we mention the types of symmetric encryption (AES) here AES-256 is the most common standard in UAVs. This standard is high-performance and optimized for application in small-sized UAVs. Asymmetric encryption (RSA, ECC) is used for more secure key exchange. Elliptic Curve Cryptography provides the same level of security as smaller keys and saves resources.

Various encryption technologies can be applied for UAVs with the proposed block tool. If we mention the types of symmetric encryption (AES) here AES-256 is the most common standard in UAVs. This standard is high-performance and optimized for application in small-sized UAVs. Asymmetric encryption (RSA, ECC) is used for more secure key exchange. Elliptic Curve Cryptography provides the same level of security as smaller keys and saves resources. In addition to those mentioned, the completeness of the information must be ensured. For this, HMAC (Hash-Based Message Authentication Code) technology is applied. This technology confirms that the data sent has not been changed. Hash functions such as SHA-256 or SHA-512 are used here [4].

Regarding coding protocols, it can be noted that it is intended that the data coding method will be applied in protocols such as MAVLink for compact and effective data transmission. Both high performance and flexibility are provided when the implementation of coding and encryption block realization is carried out with software and hardware. With software (Software-based), algorithms such as AES, RSA, or ECC are applied at the previously mentioned software level. These methods are more flexible, but inferior in performance to hardware-based encryption. With hardware (Hardware-based), chips such as TPM (Trusted Platform Module) or HSM (Hardware Security Module) which are used. This method ensures that data is encrypted with higher performance and more securely. The implementation of FPGA or ASIC-based encryption blocks is envisaged. It is necessary that navigation, communication, and control information, as well as the images obtained-in short, all-important information that affects the security of the UAV, enter the coding and encryption block.

One of the drawbacks is the existence of resource constraints. Encryption and encoding should use the computing resources of the device to a minimum. Because it is important to minimize delays. Delays are unacceptable, as processes are carried out in real time. It should be borne in mind that strong encryption and encoding algorithms require more resources. The proposed systems must be resistant to radio-electronic obstacles.

3.1.4. Comparison and generation block

A comparison and generation signal broadcasting block is intended to be used as part of a system against attempts to seize control or fraudulent navigation. This module tracks the true coordinates of the UAV and generates false signals against external threats. The initial function of the mentioned block is the comparison of the received, benchmark, and generated false coordinates. As a benchmark, the most appropriate coordinate of the UAV is considered to perform the assigned task. Benchmark coordinates tend to match the flight plan; however, current coordinates may not always match benchmark coordinates. It receives the current coordinates of the UAV through the built-in inertial navigation system (INS) and GPS. It also compares this data with the benchmark route stored in the system's memory. To confuse the enemy side, it creates and transmits false coordinates, different from the current benchmark and current coordinates. The signal is not broadcast when the error is detected. For example, data is not sent to the transmitter if the created coordinate matches the benchmark or current location.

The module can be executed on the example of general-purpose processors with comparison algorithms, such as STM32. Because the block implements the processing logic after obtaining GPS coordinates, INS data, and a benchmark route (a planned route previously stored in memory). At this step, the comparison algorithm comes into play. Taking into account the pattern of movement at the output of this block, false coordinates are created, and misinformation is sent to the transmitter (translator of false signals) of false signals through interfaces such as UART, SPI, or CAN.

When emitting false signals and transmitting false object, there must necessarily be a block of comparisons so that the coordinates of the fake targets applied by chance and the real UAV are not the same. At present, the management of the UAV and other tactical actions cannot be entrusted to artificial intelligence, since the security of the information subject is not fully ensured.

However, if the security required by this method is ensured and the management issues go to a completely new stage, it will already be possible to develop more flexible and highly maneuverable UAVs through the use of artificial intelligence [10].

3.1.5. Data storage block

To create a system that is resistant to cyber threats, it is necessary to adhere to the main triad in the exchange of information. The triad means that information is confidential, integral and, available (CIA). For this reason, information must necessarily be stored, and memory devices are available for this. The memory device allows telemetry and reading of flight records from the database only after identification. It is because of the memory device that information remains accessible to the on-site management staff and other services [5].

The main role of the memory device in the exchange of information is shown in Fig. 2.

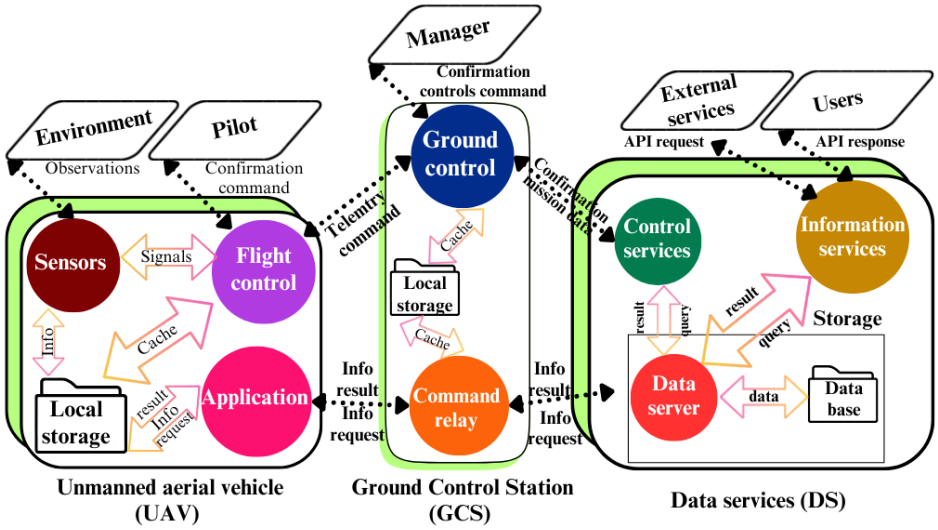

Fig. 2. Data Flow Diagram (DFD) for the UAV

In the proposed module, local memory is used for temporary storage of incoming data. The memory should be high-speed and reliable, for example, based on eMMC or NVMe. The memory device can be used as a kind of redundant system in the future. It can be used as an additional layer of protection to create backup copies of key data and limit attackers' access to the system. The distribution block of protected information manages the transmission of encrypted information. From here, information is transmitted to control surfaces, autopilot and, if necessary, to other channels.

4. ALGORITHM DEVELOPMENT

For the exact functionality of the proposed complex method, in addition to the specific work algorithm of the modules and elements, there must be a special algorithm of the general UAV. Through the special algorithm, coordination will be established between the elements and systems, and the information exchange will occur in accordance with the sequence we have determined. The algorithm shown in Fig. 3 has been constructed for the implementation of the proposed method.

To protect the UAV, especially its avionics systems, from cyber threats, very effective information exchange must be implemented. When developing this algorithm, it is necessary to consider several main factors. Information must be distributed and transmitted quickly across all channels. Blocks that are most likely to fail must be integrated in a special way. More

precisely, the re-entry of these blocks into the cycle must be organized as soon as possible. Since current UAVs are functional, the data flow can be large. In addition, due to certain reserves, the number of data transmission buses may be excessive. Taking all of this into account, the development of the algorithm should be as simple as possible. The simplicity of the algorithm will prevent the system from being overloaded.

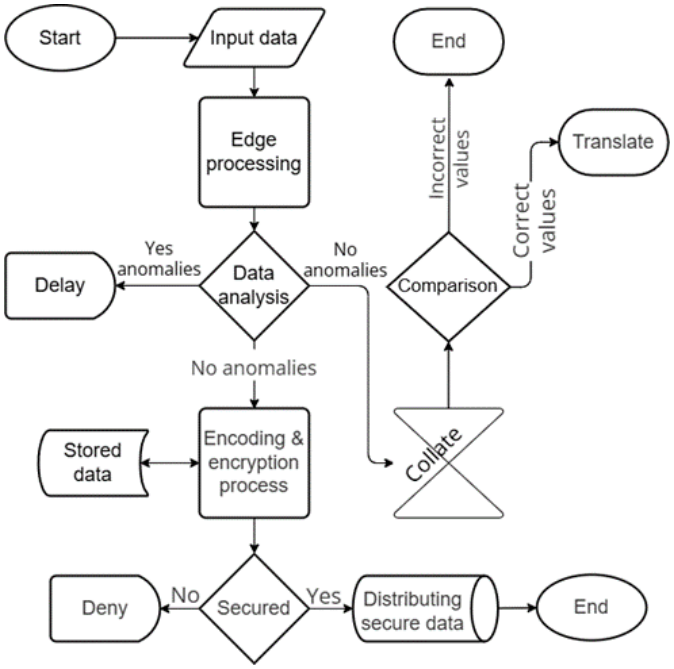

Fig. 3. Data Flow Diagram (DFD) for the UAV

The process of sequencing information received from transmitters and other channels is reflected in the algorithm. After the integrated elements and blocks, we can see the principle of operation of the system in this algorithm. The received information is first sent to the edge processing block. UAVs are equipped with various transmitters (GPS, accelerometer, gyroscope, barometer, cameras, etc.). Altitude, speed, direction and position information is received from the transmitters. The processing block collects the information received from the mentioned transmitters and stores it in the correct format. Position data is necessary for navigation and tracking the path.

To ensure that UAVs fly the correct route, the processing unit monitors the position and movement of UAVs based on GPS data and other navigation systems. This ensures that the flight plan is executed correctly. The comparison and generation block analyzes information about the flight plan, current coordinates and produces new values for transmitting coordinates. When comparing and generating coordinates, this block will use the Haversine formula and spherical trigonometric formulas.

$$a = sin^2 + \left(\frac{\Delta\phi}{2}\right) + cos(\phi_1) \cdot cos(\phi_2) \cdot sin^2(\frac{\Delta\lambda}{2}) \tag{1}$$

$$c = 2 \cdot arctan2(\sqrt{a}, \sqrt{1-a}) \tag{2}$$

$$d = R \cdot c \tag{3}$$

Where:
ϕ_1, ϕ_2: latitudes of the two points in radians;
λ_1, λ_2: longitudes of the two points in radians;
$\Delta\phi = \phi_2 - \phi_1$: difference in latitude;
$\Delta\lambda = \lambda_2 - \lambda_1$: difference in longitude;
R: radius of the Earth (mean value is approximately 6,371);
d: great-circle distance between the two points.

Spherical trigonometry deals with the relationships between angles and arcs on a sphere, often used in navigation. Below are the basic formulas of spherical trigonometry that are used in the generation of coordinates.

Law of cosines for distance:

$$\cos(a) = \cos(b)\cos(c) + \sin(b)\sin(c)\cos(A) \tag{4}$$

Law of cosines for angles:

$$\cos(A) = -\cos(B)\cos(C) + \sin(B)\sin(C)\cos(a) \tag{5}$$

Law of sines:

$$\frac{sin(a)}{sin(A)} = \frac{sin(b)}{sin(B)} = \frac{sin(c)}{sin(C)} \tag{6}$$

Using these formulas, we can calculate distances and bearings between two points on the globe.

The presented algorithm allows providing a high level of protection against external interference. In addition, the integration of the coding, encryption block, as well as the implementation of the comparison and false signal generation module somewhat complicates the task of the system. In such a case, a special algorithm is necessary to exclude errors.

5. CONCLUSION

Referring to the conducted research, it can noted that the article touches on very important nuances. The proposed complex approach combines encryption, coding operations, and the dissemination of fake information during data exchange and can be easily implemented. In this process, no serious changes are made to the main systems of UAVs. Only the required modules are connected to existing equipment, and interfaces are adapted. The implementation of this approach can bring UAVs to a new stage of development. Many currently available digital solutions are not used due to security problems. Thanks to the integration of the proposed modules, it is possible to ensure security and remove existing restrictions. If we minimize the risk of cyber-attack threats with the proposed methods, UAVs can move to a new level of development in the future. In this case, we can achieve more functionality of UAVs by applying artificial intelligence and other new technologies.

References

1. Chen C.L., Y.Y. Deng, W. Wang, C.H. Chen, Y.J. Chiu, C.M. Wu. 2020. "A traceable and privacy-preserving authentication for UAV communication control system". *Electronics* 9(1). DOI: 10.3390/electronics9010062.
2. Hassanalian M., A. Abdelkefi. 2017. "Classifications, applications, and design challenges of drones: A review". *Progress in Aerospace Sciences* 91(4). DOI: 10.1016/j.paerosci.2017.04.003.
3. Hong Young-Woo, Dong-Young Yoo. 2024. "Multiple Intrusion Detection Using Shapley Additive Explanations and a Heterogeneous Ensemble Model in an Unmanned Aerial Vehicle's Controller Area Network". *Applied Sciences* 14(13): 5487. DOI: 10.3390/app14135487
4. Cui J., Y. Chen, H. Zhong, D. He, L. Wei, I. Bolodurina, L. Liu. 2023. "Lightweight encryption and authentication for controller area network of autonomous vehicles". *IEEE Trans. Veh. Technol.* 72(11): 14756-14770.
5. Sion L., K. Yskout, D. Van Landuyt, A. van den Berghe, W. Joosen. 2020. "Security Threat Modeling: Are Data Flow Diagrams Enough?". 2020. In: *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. New York, NY, USA, p. 254-257. DOI: 10.1145/3387940.3392221.
6. Oded Vanino, Dikla Barda, Roman Zaikin. November 8, 2018. "DJI Drone Vulnerability". Available at: https://research.checkpoint.com/2018/dji-drone-vulnerability/?utm_source.
7. Sihag Vikas, Gaurav Choudhary, Pankaj Choudhary, Nicola Dragoni. 2023. "Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next Generation Drones". *Drones* 7(7): 430. DOI: 10.3390/drones7070430.
8. Simon Niyonsaba, Karim Konate, Moussa Moindze Soidridine. 2023. "A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions". *International Journal of Computer Networks and Applications (IJCNA)* 10(5): 688-705, DOI: 10.22247/ijcna/2023/223417.
9. Sofiane Zaidi, Mohammed Atiquzzaman, Carlos T. Calafate. 2021. "Internet of Flying Things (IoFT): A Survey". *Computer Communications* 165: 53-74. DOI: 10.1016/j.comcom.2020.10.023.
10. Tlili F., S. Ayed, L.C. Fourati. 2024. "Advancing UAV security with artificial intelligence: a comprehensive survey of techniques and future directions". *Internet of Things* 27: 101281. Doi: 10.1016/j.iot.2024.101281.
11. Zeng Y., R. Zhang, T.J. Lim. 2016. "Wireless communications with unmanned aerial vehicles: opportunities and challenges". In: *IEEE Communications Magazine* 54(5): 36-42. DOI: 10.1109/MCOM.2016.7470933.
12. Yu Z., Z. Wang, J. Yu, D. Liu, H.H. Song, Z. Li. 2024. "Cybersecurity of Unmanned Aerial Vehicles: A Survey". *IEEE Aerospace and Electronic Systems Magazine* 39(9): 182-215. DOI: 10.1109/MAES.2023.3318226.

Received 28.01.2025; accepted in revised form 10.04.2025