https://www.proconference.org/index.php/usc/article/view/usc24-00-002
DOI: 10.30888/2709-2267.2024-20-00-002

UDC 004.056

USAGE OF UNMANNED AERIAL VEHICLES FOR OBJECT MONITORING AT CRITICAL INFORMATION INFRASTRUCTURE

Zaika Nazar
junior researcher
ORCID: 0000-0002-5791-8926
Komarov Maksym
c.t.s
ORCID: 0000-0002-5739-8959
Ishchuk Maksym
ORCID: 0009-0008-1132-8665
Verkhovets Oleksii
ORCID: 0000-0002-3897-106X
State Research Institute of Cyber Security Technologies, Kyiv,
M. Zaliznyaka Street, building 3, bloc 6, 03142

Abstract. *The article explores the importance and challenges of ensuring the security of critical information infrastructure (CII). It explains that this includes managing situations of emergency character, physical security systems, and the use of unmanned aerial vehicles (UAVs) to enhance security. The technical aspects of security systems, such as radio navigation systems, navigation, and aerial reconnaissance systems, are described in detail. Practical recommendations are provided to enhance the protection of critical infrastructure objects from cyber attacks and other threats.*

Key words: *Security, critical infrastructure, emergency management, unmanned aerial vehicles, radionavigation, cybersecurity.*

Introduction

Ensuring the security of critical information infrastructure objects (hereinafter referred to as CIIO) aims to prevent violations of their integrity and safety. Managing emergency situations, such as diversions at CIIO, is a complex process that can be addressed by breaking down functions and assessments into specific boundary values. Studying boundary values to identify extremes enables the determination of optimal solutions for effective emergency situation management [1].

The physical security system of CIIO encompasses a range of measures, including organizational procedures, engineering tools, and actions by security and safety units aimed at ensuring the internal regime of the facility. The primary technical component of such a system is a complex of engineering tools based on an automated integrated security system. This complex includes visual, radar, and acoustic detection devices, video surveillance systems, communication systems, aerial reconnaissance, engineering barriers, and comprehensive information security

systems. The fundamental principle of this system is the principle of prevention, meaning that the faster a threat of intrusion onto the facility is detected using detection means, the more effectively the problem will be addressed [2].

The advantage of using radar systems for monitoring lies in their ability to gather information about the surrounding environment at any time, regardless of the time of day, weather conditions, natural phenomena, pollution levels, or radiation exposure. Modern technologies enable the collection of a large amount of data about the state of the surrounding environment [3]. However, it is important to consider the challenges associated with isolating the useful signal against the background of stationary obstacles and the influence of atmospheric conditions on radar emissions during contamination. It is also necessary to consider the technical aspects of methods for isolating the useful signal against the backdrop of obstacles. Additionally, it is important to consider the possibility of target masking and the presence of additional objects near the primary target. Taking into account the information risk when assessing threats involves applying an algorithm for quantitatively assessing the risk of information loss [4].

Usage of Unmanned Aerial Vehicles (UAVs) for Object Monitoring

Unmanned aerial vehicles (UAVs), equipped with numerous sensors and advanced processors, are capable of rapidly collecting vast amounts of information. Security experts must understand the principles of UAV operation, analyze their technical specifications, and determine their locations. They should also participate in developing response plans for the unauthorized use of UAVs over the company's premises, detailing the steps necessary to mitigate the risk of an event or incident in accordance with current legislation.

UAVs provide the capability to obtain real-time aerial imagery, which can be directly transmitted to ground personnel. This allows security personnel to make more informed decisions both in emergency situations and during routine patrols. The use of UAVs for security purposes enables investigations to be conducted without risking the safety of a crew. Additionally, UAVs are utilized for threat detection during territory monitoring and environmental status tracking.

Automation of UAVs in Security and Surveillance

Technologies of automation are applied for industrial and commercial security purposes. One of the most significant factors influencing the growth of the automated security systems market is the availability of software as a service that can operate independently of specific hardware. It is precisely the software that defines the direction of autonomy and automation development, which are governed by the functionality of Unmanned Aerial Vehicles (UAVs) for surveillance [5].

Reconnaissance and Surveillance

UAVs can provide real-time footage and data from a unique perspective, offering unique opportunities for threat assessment and informed decision-making. UAVs can conduct reconnaissance and surveillance to fulfill the security needs of an enterprise, and the addition of thermal cameras with enhanced zoom capabilities allows for the detection of hidden objects or individuals even in limited visibility conditions. For instance, drones can help detect mines on roads or in fields and identify the presence of individuals inside buildings based on their thermal signatures. This means that surveillance drones can provide reliable information about the precise location, position, and direction of movement of living objects [6].

Mapping and Mission Planning

Having real-time data from unmanned aerial vehicles (UAVs), highly accurate maps can be created for strategic planning purposes. Mapping drones assist in visualizing and georeferencing any external environment that is likely to be utilized for the security system of an object. This is particularly useful when high precision is required, such as during the mapping of hazardous road sections. With these devices, large territories can be scanned, and digital terrain models and 3D maps can be created for further strategic planning, logistics, and execution of other tasks related to territory monitoring and facility surveillance.

Emergency control systems

After natural disasters or conflict situations, unmanned aerial vehicles (UAVs) can be utilized to provide urgent assistance and support. They conduct surveillance of the surrounding environment, providing crucial information to plan routes, rapidly

detect and respond to hazardous situations, and coordinate rescue operations. UAVs equipped with infrared sensors can detect heat signatures of living beings under debris, allowing rescue teams to more effectively locate those in need of assistance. Additionally, they can deliver medical equipment, food, and other essential items or assess damages and identify areas requiring assistance.

Robotic intrusion detection

Robotic systems can be programmed to automatically respond to detected intrusions or to send alerts and signals for further analysis and processing by human operators. This approach can be applied in various domains, including security, manufacturing, healthcare, and others.

In the event of an intrusion, aerial surveillance data can also serve as evidence. Video footage not only is transmitted but also documented, providing authentic and clear records for insurance claims. By integrating innovations into the intrusion detection domain, our system offers robotic intrusion detection. Notifications are intelligently sent only after the detection of human and vehicular intruders. This strategic approach ensures timely and effective notifications, enhancing the efficiency and effectiveness of security measures [7].

For remote monitoring and to extend the coverage area for protecting information systems and countering cyber threats, modern unmanned aerial vehicles (UAVs) are utilized. Multirotor UAVs are particularly popular due to their design and mobility, allowing them to maneuver and perform complex tasks in both forested areas and urban environments. They can operate autonomously and be controlled without operator intervention.

Navigation systems for positioning unmanned aerial vehicles

It is worth noting that conventional navigation and positioning systems, such as satellite navigation, do not work indoors. The signal strength through concrete and metal structures for UAVs is weak. Therefore, local radio navigation systems, optical-beam systems, or systems using computer vision are employed. To prevent data theft, some UAVs are designed without external signal receivers. It is important to mention that this approach is quite complex to implement, as it requires

synchronous operation of the UAV modules and coordinated operation of the ground station robotic complex. This means that the only device periodically connected to the UAV is the ground docking station. This simplifies data security protection. Selecting the right software for the monitoring system is an important aspect from the perspective of cybersecurity.

If there is no map of the space, and obstacles may be encountered along the UAV's path, such as people, cars, and other infrastructure objects, the UAV should be equipped with special devices for detecting such obstacles. For example, ultrasonic and laser rangefinders or stereo cameras can be installed, allowing for the localization of objects in the UAV's path and the construction of a map of the building or surrounding environment. If we are talking about monitoring warehouses, the UAV's camera can also be equipped with a special QR code scanner for checking and inventorying products and goods stored in the warehouse.

Considering that there may be no lighting inside the premises, the UAV should be equipped with special floodlights or sensors whose operation is not dependent on the level of illumination for orientation inside the premises. Algorithms based on spatial measurements from sensors are necessary for constructing a map of the space in an unknown environment. The UAV should plan the optimal route, taking into account the flight time limitations due to the battery charge level.

The development of UAV modernization solutions is carried out using simulation modeling, where flight algorithms are first tested in a simulator and then applied to a real device.

Multirotor UAVs are the most well-known UAVs. The power components of these devices include an engine, propeller, and drive, which work together to provide the lift and movement of the aircraft in the air. Control systems, controllers, and regulators are used for effective control of power components. These devices allow controlling the angular velocity of the engines and the position of the drive, ensuring stable and precise operation of the UAV [8].

The tasks are related to the coordination of a large number of devices

To control a group of UAVs performing various aerobatic maneuvers, such as

LED flashing to create spectacular aerial displays, a control program needs to be developed for each aircraft, followed by pre-flight testing. During flight, the aircraft can form both simple geometric shapes and complex animations. Simulation modeling systems allow for the calculation of all flight trajectories, from takeoff to landing, and assess the feasibility of executing the flight program considering the characteristics of the aircraft and their flight time.

During flight, the distance between aircraft when forming figures can be just a few dozen centimeters, so it's essential to have a navigation system with centimeter-level accuracy. For takeoff and landing, when the accuracy of the navigation system may be insufficient, the aircraft take off in small groups. In indoor environments for group flights, special local positioning radio navigation systems can be used, along with other systems with a similar operating principle. A crucial aspect is synchronizing the group of aircraft, for which a temporary scale of the navigation spacecraft with a highly accurate atomic clock is utilized.

Recommendations

To enhance resilience against cyber attacks on state information resources and critical infrastructure objects, the following recommendations are proposed:

1. Develop personnel capacity and ensure proper oversight of cybersecurity for critical information infrastructure objects. This entails studying and implementing cutting-edge technologies and protection methods against cyber threats.

2. Establish specific requirements for physical security systems, vulnerability assessments of objects, probability of harm assessment, physical security system checks, comprehensive information security systems, and interaction plans.

3. Conduct measures to assess employees' awareness of cybersecurity rules and contemporary cyber threats. This may include testing knowledge and skills in cybersecurity, as well as providing educational materials and instructions for staff.

Conclusions

The utilization of modern technologies for protecting critical information infrastructure objects significantly expands capabilities in the domains of tracking, monitoring, automation, and enhancement of comprehensive data security systems.

Analyzing information during environmental monitoring involves identifying potential threats, determining their parameters and level of risk, as well as implementing risk reduction methods and preventing potential issues, along with continuously monitoring the situation. This is a crucial stage in ensuring the security of information resources.

References

1. Dyvizinyuk M., Miroshnyk O., Ryzhkin O., Borodina N., Rybka Y. Solving boundary problems as a way to assess the effectiveness of managing an emergency situation of a terrorist nature at a critical infrastructure facility. *Legal, regulatory, and metrological support of the information protection system in Ukraine*. 2017. Vol. 2 (34). P. 89 – 98.

2. Azarenko O., Honcharenko Y., Lazarenko S., Oyganova M., Siotenko O., Kasatkina N., Kachur T. Mathematical model for detecting dangerous targets on approaches to critical infrastructure objects in complex hydrometeorological conditions and in the presence of stationary masking obstacles. *Legal, regulatory, and metrological support of the information protection system in Ukraine.* 2017. Vol. 2 (34). P. 99 – 107.

3. Skachek L. M. The value of information in information security. *Information Security*. 2003. Vol. 3(9). P. 52–54.

4. Honcharenko Y.O. Choosing an approach to assessing information security risks for retail companies: master's thesis. Kyiv, 2019. 92 p.

5. Drone Autonomy software platform developed for system integrators. https://www.flytbase.com/security-and-surveillance

6. Aerial reconnaissance with unmanned aerial observation. https://www.deltaquad.com/vtol-drones-for/security-and-defence

7. Aerial reconnaissance with unmanned aerial observation. https://www.nightingalesecurity.com

8. Security and critical infrastructure. https://dronehub.ai/defence-security

Scientific adviser: c.t.s, Komarov M.U.

sent: 18.04.2024 © ZaikaN.V.