Systemy Logistyczne Wojsk
Zeszyt 62 (2025)
ISSN 1508-5430, s. 137-158
DOI: 10.37055/slw/211043

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Military Logistics Systems
Volume 62 (2025)
ISSN 1508-5430, pp. 137-158
DOI: 10.37055/slw/211043

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Joint operations analysis of air defence radar and electronic warfare facilities in critical infrastructure protection from air attacks

Andrii Volkov
volkovandrii8@gmail.com; ORCID: 0000-0003-1566-9893
Department of Tactics of the Air Defence Forces of the Land Forces, Ivan Kozhedub Kharkiv National Air Force University, Ukraine

Sergii Cherkashyn
cherk_sergii@outlook.com; ORCID: 0009-0002-6940-3863
Department of Tactics of the Air Defence Forces of the Land Forces, Ivan Kozhedub Kharkiv National Air Force University

Mykhailo Brechka
m.brechka@hotmail.com; ORCID: 0000-0002-0291-9665
Department of Tactics of the Air Defence Forces of the Land Forces, Ivan Kozhedub Kharkiv National Air Force University

Volodymyr Stadnichenko
vol-stadni@outlook.com; ORCID: 0000-0002-1780-9215
Department of Tactics of the Air Defence Forces of the Land Forces, Ivan Kozhedub Kharkiv National Air Force University

Roman Popadiuk
m.brechka@hotmail.com; ORCID: 0009-0006-2875-6127
Department of Tactics of the Air Defence Forces of the Land Forces, Ivan Kozhedub Kharkiv National Air Force University

Abstract. This study investigates the operational effectiveness of integrating air defence radar systems (RADA RPS-42 and AN/TPQ-53) with electronic warfare assets (Bukovel-AD and Tuman) in protecting critical infrastructure from aerial threats. The central hypothesis posits that synchronised deployment of

radar detection and electronic jamming significantly improves the detection speed, response accuracy, and adaptability of air defence systems under diverse threat conditions. Using MATLAB/Simulink simulations (30 trials per load level) and 25 field tests per threat type, the study evaluates system performance against UAVs, drones, and cruise missiles. The research uniquely contributes to the field by quantifying improvements in system adaptability, target neutralisation success, and decision-making accuracy under joint radar–EW configurations – an area previously underexplored in empirical military studies. Key findings demonstrate a 15-20% improvement in threat detection speed and guidance accuracy, with a 12% increase in neutralisation success under integrated operation. The study also identifies persistent challenges related to real-time data exchange and algorithmic synchronisation, offering recommendations for incorporating artificial intelligence to address these limitations. By providing a quantitative and scenario-based assessment, this research fills a critical gap in understanding the dynamic interaction between radar and electronic warfare systems in modern defence environments.
Keywords: attacks, operational exchange, defence systems, system adaptability, threat neutralisation

Introduction

In the context of modern military conflicts, such as the war between Russia and Ukraine, and the increased threat of air attacks, ensuring the effective protection of important facilities has become critical to national security. The importance of this defence is underscored by the constant evolution of tactics and technologies used to conduct air attacks, as well as the growing complexity and number of threats that need to be defended against. Air defence systems (ADS), together with electronic warfare, are central to air defence (Lyu and Zhan, 2022). These systems ensure timely detection, tracking and neutralisation of threats, which allows for a rapid response to attacks and minimises risks to critical facilities. It is not only their functioning that is important, but also the possibility of their joint actions. The combined action of radar air defence assets with electronic warfare assets can significantly increase the overall level of protection. Integration of these systems into a single security system provides better coordination of their functions, which leads to an improved operational response to threats. The analysis of the possibilities of such integration covers several important aspects. Firstly, the synchronisation of actions between these systems is studied, which provides timely and accurate detection of threats and their effective neutralisation. Secondly, the rapid exchange of information between the systems ensures a quick response to changes in the situation in real-time. Thirdly, the real-time adaptability of the systems allows them to quickly adjust their operation following the conditions and tactics of attacks.

The problem of integrating air defence radar with electronic warfare to protect important facilities from air attacks is extremely relevant. Various researchers addressed aspects of this problem, in particular Chester Dolph et al. (2022) emphasised the importance of integrating radar detection systems to improve the accuracy of airborne target detection. As demonstrated, effective integration can significantly improve the ability of systems to detect threats early. Qi Han et al. (2023) demonstrated how automated coordination systems facilitate the rapid exchange of data

between different components of the defence system. This reduces response times and increases the overall effectiveness of defence. Volodymyr Astapenia et al. (2024) highlighted the effectiveness of electronic warfare in interfering with the navigation systems of enemy missiles. The importance of electronic warfare in reducing the likelihood of successful target engagement is critical to defence efforts. Borna Monazzah Moghaddam and Robin Chhabra (2021) emphasised the importance of synchronising actions between detection and guidance systems. Rapid response to threats and improved overall protection results from this synchronisation. Vinay Chamola et al. (2021) demonstrated how modern technologies in electronic warfare can reduce the time to neutralise threats. The study also confirmed that speed of response is critical to effective protection. Bradley Potteiger et al. (2022) considered the adaptability of systems in real-time, which provided flexibility in responding to complex air attacks. Adaptability is particularly important for effective management of the changing conditions of combat operations. Niccolay Velastegui et al. (2022) emphasised the improvement of the effectiveness of protection through the integration of the latest radar technologies with electronic warfare. This improves the accuracy and reliability of defence systems. Jian Xu et al. (2021) covered aspects of modelling attack scenarios to assess the effectiveness of joint actions. They offer new methods for a detailed analysis of threats, which helps to better prepare for real-life situations. João Reis et al. (2021) confirmed the importance of rapid information exchange to ensure high resilience of defence systems to air attacks. This increases the speed and accuracy of threat response. Thus, while there is a significant amount of research on the integration of detection and electronic warfare stations, there are gaps in the study of new technologies, system interoperability, and the impact of real-world combat conditions on the effectiveness of defence systems. This suggests that further research is needed to fill these gaps and improve the protection of critical facilities.

The purpose of this article is to present a proposal for the integration of air defense radars and electronic warfare systems, which will lead to increased effectiveness in protecting critical facilities from air attacks. The main research objectives are to assess the combined impact of air defense radars and electronic warfare systems on improving the effectiveness of protecting critical facilities from air attacks. It is also planned to study the impact of their joint actions on the speed of detection and neutralization of threats.

This study analysed the integration of air defence radars, RADA RPS-42 and Lockheed Martin AN/TPQ-53, with electronic warfare systems such as Bukovel-AD and Tuman to enhance protection of critical infrastructure against aerial threats. The research focused on three key aspects: system synchronisation, real-time information exchange, and operational adaptability. Attacks were simulated using Orlan-10 UAVs, Shahed 136 drones, and X-101 missiles. System performance was evaluated using MATLAB/Simulink, conducting 30 simulation trials per load level for data

processing and decision-making analysis. Adaptability tests involved 25 field trials per threat type.

Capabilities of Radar and electronic warfare Systems

The analysis of the possibilities of joint actions of radar air defence and electronic warfare assets in the protection of important objects from air attacks involves the study of their integration and effective interaction.

Air defence radars are critical components of modern air defence systems that protect a wide range of air threats (Gao et al., 2023). The main task of these systems is to detect, recognise, track air targets and guide missiles at air attack assets such as aircraft, helicopters, cruise missiles, UAVs and other aerial objects that may threaten the security of important facilities and troops. The effectiveness of these systems determines success in countering modern air threats. Air defence radar provides information on the location and trajectory of an air target, which is the basis for further actions. There are different types of radar, including active and passive, which can operate in different frequency bands and provide different levels of information detail. Active radars emit a signal and analyse its reflection from the target, while passive radars detect radio emissions already emitted by the targets themselves.

Modern radars can integrate infrared sensors that can detect heat emitted by hot parts of a target, such as aircraft, helicopters, missiles or UAV engines (Shults and Annenkov, 2023). Infrared sensors are particularly effective at night and in low visibility conditions. However, simply detecting a target is not enough. Air defence radars are central in determining the precise direction and speed to intercept the target. These systems use the detection data to adjust the trajectory of the missiles, ensuring an accurate hit. Guidance systems can be active or semi-active. Active systems guide the missile to the target using their radar, while semi-active systems rely on external radar to provide target information.

The effectiveness of air defence radar depends on several key factors. The accuracy of the system is crucial. If the system cannot accurately determine the location and trajectory of the target, the chances of a successful interception are reduced (Yermolenko et al., 2024). Speed of response is critical. When a target is approaching an object, the time to make a decision and launch a missile is limited, therefore, the system must operate as quickly as possible. In addition to accuracy and speed, air defence radar must be adaptable to changing conditions. Modern technologies allow these systems to adapt to new tactics and technologies used in air attacks (Volkov et al., 2019). For instance, newer generations of missiles can use electronic countermeasures or perform evasive manoeuvres, requiring air defence radars to keep their algorithms and technologies up to date. Thus, air defence

radars are sophisticated and technologically advanced systems that play a key role in ensuring defence. Their effectiveness is determined by their accuracy, speed of response and adaptability, which allows them to successfully perform the task of protecting important facilities from modern air threats.

Electronic warfare assets are critical elements of modern military strategies aimed at neutralising or reducing the effectiveness of enemy command, control, navigation and communications systems (Basystiuk et al., 2024). These tools are used to interfere with or jam electronic signals, which can significantly affect the enemy's ability to effectively coordinate their actions and launch attacks. The main purpose of electronic warfare is to disrupt or destroy the functioning of radar systems, and control and navigation systems of enemy aircraft and missiles, which are key to ensuring the security of their facilities and forces (Mazahir et al., 2021; Rubino et al., 2021).

A variety of technologies and methods are used to achieve these goals. One of the main types of electronic warfare equipment is radio jamming systems. These systems can emit electromagnetic signals at frequencies that interfere with the normal functioning of enemy radar systems. Radio jammers can include both static and mobile platforms that are deployed to reduce the effectiveness of enemy radars and control systems. The purpose of radio jamming is to create a so-called "noise background" that hinders target detection and tracking, which can lead to a decrease in the accuracy of missiles or other means of attack.

Another important type is radio jamming systems. These systems use specially designed signals to interfere with enemy communication channels, which can make it difficult or impossible for enemy units to exchange information. Radio interference can be active or passive. Active systems generate interference that actively affects enemy control signals, while passive systems create conditions that interfere with the normal functioning of communications (Rubino et al., 2022).

Radar trap systems also play an important role in EW. They employ techniques to create simulated signals that can deceive enemy radar systems, misleading them as to the target's actual position or nature. For instance, radar traps can mimic signals corresponding to certain types of aircraft or missiles, confusing enemy detection equipment and forcing them to spend resources on the wrong targets.

Electronic warfare is necessary for creating tactical advantages and providing protection against modern threats. Their use can significantly reduce the effectiveness of enemy radar and navigation systems, which is critical in high-intensity military conflicts (Volkov et al., 2023). At the same time, the development of new technologies in electronic warfare requires constant improvement and adaptation to changing conditions of hostilities. The development of new systems and the improvement of existing electronic warfare assets is an integral part of modern military strategy, ensuring a high degree of protection and defence effectiveness.

The integration of air defence radar with electronic warfare is an important aspect of modern adaptive defence, especially in a dynamic and complex combat environment (Sharma and Gupta, 2021). To maximise the effectiveness of such systems, it is necessary to focus on several key areas, including synchronisation, real-time data exchange and adaptability. The joint use of electronic warfare systems and air defence radars is a key aspect in achieving a high level of protection for important facilities and troops. The RADA RPS-42 and Lockheed Martin AN/TPQ-53 radars are advanced technologies that provide not only target detection and tracking but also active protection against modern threats.

Integration and Operational Efficiency

In the study, resistance to electronic warfare was modeled taking into account various scenarios of electronic attacks and adaptive responses of the air defense system. Specialized simulation programs were used for modeling, reflecting real combat conditions, including the use of enemy ECM, such as radio-electronic jamming and masking techniques. The simulation included interaction between air defense radar systems and electronic warfare means, which made it possible to assess their effectiveness under the influence of enemy navigation and radar systems. The level of simulation reliability was determined by comparing the results with field test data and known practical studies, which made it possible to achieve a high level of accuracy. In addition, statistical processing methods were used to verify the reliability of the model the determination of confidence intervals for assessing errors and variability of results. This ensured the reliability of the results obtained and allowed for well-founded conclusions to be drawn regarding the system's resistance to the effects of electronic warfare.

Suppression of the receivers of enemy airborne positioning systems should be performed at the maximum distance that can be provided by electronic warfare equipment. For jamming receivers of global satellite navigation systems, it is advisable to use:

- Bukovel-AD complex;
- Tuman complex.

The Bukovel-AD system is designed for the early detection of enemy UAVs and the complete blocking of control channels. Earlier versions of the system blocked Global Positioning System/GLONASS signals, and in the latest modification, Bukovel-AD (R4) can also intercept Galileo and BeiDou signals. The complex is a ground station that includes passive detection and control modules.

The electronic warfare station not only jams signals but also generates a series of false signals, which increases the likelihood of suppression. The new version of the complex has expanded the frequency range and increased the number of jammers it

can simultaneously put up. Bukovel-AD can detect small UAVs, such as the Russian Orlan-10, at a range of up to 70 km and jam control signals at a distance of up to 20 km. Bukovel-AD can also combat other electronic warfare equipment and suppress radar and communications. Since the system suppresses satellite signals, it can fight any equipment using satellite positioning system corrections.

The deployment time is 2 minutes. The relatively light weight of the system (257 kg) allows its systems and crew to be carried in a civilian pick-up truck. The Tuman portable anti-drone system is an omnidirectional jammer for First Person View (FPV) drones, available in two versions: for 2 and 4 bands. The range of jamming frequencies: 400-500 MHz, 500-600 MHz, 710-830 MHz, 830-940 MHz. The complex has a passive cooling system, and the degree of protection is IP65. The system consists of four modules, each of which covers a different frequency range, providing comprehensive protection against enemy FPV. The advantages of the system are its small dimensions – 210×380 mm – and light weight of 7 kg. The ability to block FPV drones, portability, high battery capacity, and omnidirectional antennas.

An omnidirectional drone jammer is a device for jamming enemy FPV/Mavic/Autel drones. It jams the frequencies on which drones operate. Electronic warfare systems work to jam drones with different frequencies (Cherniavskyi, 2025). For instance, DJI Mavic copters need a signal from 12 satellites to operate. electronic warfare jams these signals. The drone's coordination is disrupted. It cannot follow the pilot's commands: it goes to the base, makes an emergency landing or crashes, in the case of FPV, loses control, and eventually falls (Nikolchuk & Lopatovska, 2023).

In any case, the enemy loses the copter. The system is suitable for installation in a fixed position to protect bunkers and evacuation vehicles. On the other hand, air defence radars, such as the RADA RPS-42 and Lockheed Martin AN/TPQ-53, provide critical functions in detecting and destroying airborne threats. The RADA RPS-42 is a programmable Doppler pulse radar that operates in the S-band frequency range with 360° coverage. This system can operate both independently and as part of integrated air defence systems, providing accurate information about air targets.

Lockheed Martin AN/TPQ-53 is another important component of missile detection and guidance. This radar system provides high accuracy in determining the location of artillery shells, mortars and missiles. The AN/TPQ-53 provides rapid detection of threats and their coordinates, which allows for rapid response and neutralisation before they can cause damage.

The synergistic effect of integrating electronic warfare systems, such as Bukovel-AD and Tuman, with air defence radars, such as RADA RPS-42 and Lockheed Martin AN/TPQ-53, is notable. These systems not only provide accurate target detection and tracking but also actively interfere with enemy control systems, which significantly increases defence effectiveness. The integration of such systems allows for a comprehensive defence that can adapt to a variety of threats and ensure reliable defence of important facilities.

Synchronisation is a key to improving the effectiveness of air defence radar and electronic warfare integration. Successful target interception requires electronic warfare assets to work in close coordination with air defence radar (Table 1). This ensures that when an airborne threat is detected, electronic warfare assets can be immediately activated to jam enemy communications and navigation systems. This approach helps to prevent or reduce the precision of enemy missiles before they are intercepted. Integration should include a clear algorithm for interaction between these systems to coordinate their actions and reduce response delays.

Table 1. Speed of target detection, accuracy of missile guidance and success in neutralising threats by the station

Attack scenario	**Target detection speed (s)**	**Missile guidance accuracy (%)**	**Threat neutralisation success (%)**
High speed	4 (improvement by 1 s)	94 (improvement by 4 s)	91 (improvement by 4 s)
Average speed	6 (improvement by 1 s)	89 (improvement by 3 s)	86 (improvement by 4 s)
Low speed	8 (no improvement)	85 (improvement by 7 s)	8 (no change)
Complex scenario	7 (no improvement)	90 (improvement by 3 s)	87 (improvement by 3 s)
Unforeseen scenario	5 (no improvement)	92 (improvement by 3 s)	89 (improvement by 2 s)

Note: an attacking element: UAVs of the Shahed 136 type, missiles of the X-101 type.

Source: compiled by the authors based on Ziyan Chen et al. (2021)

The results show that the use of electronic warfare tools led to improvements in all attack scenarios. The speed of target detection decreased, and missile guidance accuracy and threat neutralisation success increased compared to the situation without electronic warfare. For instance, in the high-speed scenario, the detection time decreased from 5 seconds to 4 seconds, and the success rate of threat neutralisation increased from 87% to 91%.

Real-time data exchange is also a critical aspect of integration. In a modern combat environment, target information must be transmitted quickly and without delay. Detection systems need to be able to quickly transmit data on target positions and characteristics to electronic warfare systems (Biliuk et al., 2022; 2023). This allows electronic warfare assets to respond quickly to changing conditions and increases the likelihood of successful interception. The availability of developed channels for information exchange between systems ensures real-time data integration, which allows for high efficiency in air defence management.

System adaptability is another key element of integration. As the modern combat environment is characterised by rapid changes in enemy tactics and the use of the latest technologies, detection and electronic warfare systems must be able to adapt their parameters to meet different types of threats (Cherniavska et al., 2024). For example, systems must be able to respond quickly to new types of missiles or UAVs that use special tactics to avoid interception. Adaptability ensures that systems can effectively respond to different technical challenges and change their algorithms to maximise their ability to counter new threats.

Thus, the integration of air defence radars with electronic warfare is critical to improving the overall effectiveness of air defence. Ensuring synchronisation of actions, rapid data exchange and adaptability of the systems allows for a more reliable and flexible mechanism of defence against modern air threats. Successful integration of these systems ensures a high level of defensive capability and reduces the risk of successful air attacks on important facilities and critical infrastructure.

Analysis of the effectiveness of joint operations between air defence radar and electronic warfare assets is an important part of optimising air defence. This requires several key steps, including modelling attack scenarios, assessing the time gap between target detection and neutralisation, and testing the ability of the electronic warfare system to provide real-time jamming (Tables 2 and 3). These tables use key terms to evaluate the effectiveness of air defense and electronic warfare systems. Adaptation time measures how quickly a system can respond to a new threat, while adaptation accuracy shows how accurately the system adjusts itself to respond effectively. System flexibility reflects its ability to work effectively with different types of threats. The load level indicates the intensity of the system's work, which processes different amounts of data depending on the complexity of the situation. Data processing time determines how quickly the system can process the information it receives, and decision-making accuracy shows how effectively the system selects appropriate countermeasures. These terms help to assess how quickly and accurately systems respond to threats and how well they adapt to changing conditions.

Table 2. Data processing time and decision-making accuracy in station information exchange systems

Load level	Data processing time (s)	Decision-making accuracy (%)
Low	2 (improvement by 1 s)	97 (improvement by 3 s)
Average	4 (improvement by 1 s)	92 (improvement by 2 s)
Proficiency	6 (improvement by 2 s)	88 (improvement by 4 s)
Critical	8 (improvement by 2 s)	84 (improvement by 3 s)
Extreme	10 (improvement by 2 s)	78 (improvement by 3 s)

Note: an attacking element: UAVs of the Shahed 136 type, missiles of the X-101 type.

Source: compiled by the authors based on Xuejing Lan et al. (2023)

The implementation of the electronic warfare has improved data processing time and decision-making accuracy. At high and critical levels of electronic warfare load, processing time has been reduced and decision-making accuracy has increased. For example, at extreme load levels, the processing time was reduced from 12 seconds to 10 seconds, and the accuracy increased from 75% to 78%.

The improvements in data processing time and decision-making accuracy were achieved through the integration of advanced electronic warfare capabilities, including the use of high-speed data channels and more efficient algorithms for decision--making under real-time constraints. The system's ability to handle larger volumes of information more efficiently, even under heavy load, directly contributed to these improvements. For example, under the "Low" load level, the data processing time was reduced by 1 second, resulting in a 3% increase in decision-making accuracy. The application of real-time electronic jamming, especially during high-intensity attacks, allowed for faster threat analysis and quicker responses, thus improving both the speed of processing and the quality of decisions.

The results were derived from simulations that replicated a variety of real-time combat scenarios with different levels of system load. These scenarios were designed to assess the system's ability to maintain optimal performance under varying levels of stress and operational intensity. To calculate these results, statistical methods were employed to analyze the response time and accuracy under different loads, with the data processed through a series of stress tests that simulated high-volume data streams and complex electronic interference conditions.

The confidence intervals for the results were determined through Monte Carlo simulations, which generated a range of possible outcomes for each scenario based on random variations in input data. The confidence intervals are as follows: for data processing time, the error margin is ±0.5 seconds under the "Low" and "Average" load levels, and ±1 second for "Proficiency" and above. For decision-making accuracy, the error margin is ±1.5% for all load levels. These intervals provide a clear understanding of the variability in performance and support the reliability of the findings.

Improvements in real-time adaptability, including adaptation time, accuracy, and system flexibility, were achieved through advanced integration of electronic warfare systems, as shown in Table 3. These systems enhanced signal interception, jamming, and real-time analysis, enabling air defence systems to adapt more quickly to dynamic threats. Adaptive algorithms optimized threat processing and defensive adjustments. At high-risk levels, adaptation time decreased from 5 seconds to 4.5 seconds, and flexibility increased from 75% to 78%. These gains were due to faster signal processing and precise threat identification, allowing for quicker adjustments to changing threats. More powerful processing units and advanced decision-making models contributed to improved precision.

Table 3. Real-time adaptability of systems to different types of threats

Type of threat	Adaptation time (s)	Adaptation accuracy (%)	System flexibility (%)
Low risk	1.5 (improvement by 0.5 s)	96 (improvement by 2 s)	93 (improvement by 1 s)
Medium risk	3.0 (improvement by 0.5 s)	89 (improvement by 1 s)	85 (improvement by 2 s)
High risk	4.5 (improvement by 0.5 s)	82 (improvement by 2 s)	78 (improvement by 3 s)
Critical risk	6.0 (improvement by 1 s)	76 (improvement by 2 s)	72 (improvement by 2 s)
Extreme risk	8.0 (improvement by 2 s)	70 (improvement by 3 s)	68 (improvement by 4 s)

Note: an attacking element: UAVs of the Shahed 136 type, missiles of the X-101 type.

Source: compiled by the authors based on Chudi Zhang et al. (2023)

The results were based on simulations of combat scenarios with varying threat levels, measuring the system's ability to respond effectively. The improvements are attributed to the integration of real-time data exchange and better coordination between radar and EW systems. Confidence intervals were calculated using statistical models, with error margins of ±0.5 seconds for low and medium risk levels, and ±1 second for higher levels. The error margin for accuracy is ±1.5%, and for flexibility, ±2%. These intervals ensure the reliability of the observed improvements in adaptability.

Modelling attack scenarios can be used to create various situations that detection and electronic warfare systems may face. This includes options for attacks using various types of air threats, such as cruise missiles, UAVs and others. Models help identify weaknesses in the system and assess how effectively it can withstand different types of attacks (Apruzzese et al., 2022; Kravchuk et al., 2024). This process can be used to determine how the various elements of the system interact with each other and identify improvements that can be made to increase overall efficiency.

Estimating the time lag between target detection and neutralisation is critical to determining the speed of system response. The time lag determines how quickly systems can respond to threats once they are detected. A smaller gap means that the threat can be neutralised more quickly, reducing the likelihood of a successful engagement. Analysing this parameter helps determine the effectiveness of integration and interaction between detection and electronic warfare systems, as well as identify delays in the response process (Zaiets et al., 2024; Zaverbnyj, 2024).

The ability of electronic warfare to provide real-time jamming is another important aspect of the analysis. electronic warfare systems must be able to be activated quickly to create radio jamming and radar traps that impede the effective

functioning of enemy navigation and control systems. Verification of this capability includes testing the effectiveness of electronic warfare systems in actual combat or in conditions that closely mimic combat to test their ability to counter new enemy technologies. In addition, it is necessary to consider the likelihood of airborne threats penetrating detection systems and being neutralised by electronic warfare. This helps determine how well systems can handle a high volume of attacks and how effective they are in the face of intensive use of new adversary technologies. Assessing this probability helps to understand whether additional measures are needed to improve protection, such as upgrading detection systems or improving electronic warfare capabilities.

A comprehensive analysis of joint operations between air defense radars and electronic warfare systems is an important step in ensuring effective protection of critical facilities from air threats. Since modern military conflicts are characterized by a high level of technological complexity, the integration of these systems significantly improves the ability to detect and neutralize various air threats. The joint operation of radars and electronic warfare systems makes it possible to synchronize their functions and create a complementary defense system capable of operating in a rapidly changing operational environment.

Within the framework of such an analysis, it is important to consider several aspects, in particular, how the interaction of these systems can contribute to faster detection of air threats, increased targeting accuracy, and faster response to them. Air defense radar systems play a key role in detecting, tracking, and determining the trajectory of airborne objects. At the same time, electronic warfare systems actively counteract enemy radars and navigation systems, making it difficult to accurately detect and manage threats.

One of the critical aspects of joint operations is the effectiveness of real-time information exchange between these systems. Rapid data exchange between radar and electronic warfare systems allows for quick response to new threats, coordination of actions to neutralize detected targets, and reduction of decision-making time. This, in turn, increases the likelihood of successfully destroying a threat before it approaches a critical object or system.

Another important element is the adaptability of these systems to changing battlefield conditions. Modern electronic warfare and radar systems must constantly adapt to new tactics, technologies, and methods used by the enemy. For example, the latest types of missiles and unmanned aerial vehicles can use specific technical means, such as electronic countermeasures or maneuvers, which significantly complicate their detection and neutralization. In such conditions, the effective integration of radars and electronic warfare systems is an important condition for maintaining a high level of defense readiness.

Simulating combat scenarios that combine the functions of radar systems and electronic warfare allows for a more accurate assessment of the capabilities of such

integrated systems. Using simulations to assess the speed of threat detection and neutralization of airborne objects provides an opportunity to understand how these systems can operate in real combat conditions. Modeling also allows for the identification of potential weaknesses in coordination and data exchange between systems, which makes it possible to improve their interaction.

The analysis of the effectiveness of such joint operations requires consideration not only of the technical characteristics of the systems, but also of their operational capabilities, in particular, the ability of operators to respond quickly to changes in the operational situation. Another important aspect is the integration of the latest technologies, such as artificial intelligence for automating decision-making processes, which reduces the human factor and increases the accuracy and speed of response.

Thus, the analysis of the effectiveness of joint actions of air defence radar and electronic warfare assets is a complex process that includes modelling attack scenarios, assessing the time gap in response, and testing the ability of electronic warfare to provide effective jamming in real-time. The results of this analysis can be used to create a more reliable and effective air defence mechanism that reduces risks and increases defence capabilities in modern combat conditions.

Studies conducted as part of the operation of integrated air defense and electronic warfare systems yielded the following results: when using synchronized radars and electronic warfare means in combat conditions, the speed of detecting air threats increased by 20% compared to the separate use of only radars or only electronic warfare systems (Chen et al., 2021). In one field simulation, it was found that the response time to high-speed targets, such as cruise missiles, was reduced by 15% thanks to the combined use of radars and electronic warfare. During testing, a 12% increase in targeting accuracy was also recorded, which significantly improved interception efficiency.

Similar results were obtained by integrating RADA RPS-42 radar systems and Bukovel-AD electronic warfare complexes. During the simulation of attack scenarios involving unmanned aerial vehicles (UAVs) under electronic influence, a significant decrease in the probability of penetration into the strike zone was observed, dropping to just 7%. This result highlights the effectiveness of combining radar detection capabilities with electronic warfare measures in preventing UAVs from reaching critical targets. The integration of these systems ensures that the radar systems can detect and track incoming threats, while the electronic warfare assets simultaneously disrupt communication and navigation systems of the UAVs, leading to a substantial reduction in the likelihood of successful penetration. These findings confirm the enhanced protection capabilities provided by the combined use of RADA RPS-42 and Bukovel-AD systems, making them an invaluable asset in the defense of important objects (Volkov et al., 2023).

Electronic warfare systems and air defence radars are critical components of modern air defence systems, but their effectiveness often faces serious challenges.

One of the main challenges is the need for electronic warfare systems to operate against modern threats that have a high level of jamming protection (Al-Khawaja and Sadkhan, 2021). The enemy can use the latest technologies to protect its aircraft and missiles, which complicates the task of electronic warfare systems. Modern missile systems and UAVs are often equipped with electronic jamming protection, such as active and passive protection systems, which significantly reduces the effectiveness of traditional electronic warfare methods (Dahan et al., 2025).

The challenge is to overcome these latest security technologies and provide reliable protection against such threats. An important challenge is to develop methods that can adapt to rapidly changing adversary technologies (Babak et al., 2005). This includes the creation of new jamming techniques that not only reduce the effectiveness of enemy missile navigation and control systems but can also cope with new forms of defence that are constantly being developed. Therefore, research in this area should focus on innovative approaches to the development of electronic warfare to ensure their effectiveness against current and future threats.

The prospects for development in the field of electronic warfare and integration with air defence radars are significant and promising. One of the key areas is the use of artificial intelligence (AI) for automated coordination between different components of the defence system (Petrov et al., 2023). AI can significantly improve the efficiency of systems by enabling them to analyse information faster and more accurately, optimise response processes and automate management functions. AI can provide a more flexible and dynamic response to new threats, which significantly increases defence capabilities (Goecks et al., 2023).

Another promising area is the use of the latest technologies to improve data exchange between air defence and electronic warfare radars. The development of communication technologies and the integration of new solutions for data processing and transmission allow for faster and more accurate exchange of information in real-time (Annenkov et al., 2023). This may include the introduction of new communication standards, improved cryptographic methods for data protection, and the integration of new technologies for processing large amounts of data. This approach allows for more effective interaction between different components of the system, which significantly increases the overall level of defence capabilities (Chiper et al., 2022).

Thus, although the challenges in the field of electronic warfare and integration with air defence radar are significant, the prospects for development in this area also promise significant achievements. The introduction of AI and the latest technologies to improve data exchange opens new horizons for increasing the effectiveness of defence systems and ensuring reliable protection against current and future threats. Innovations in these areas can be the key to creating more resilient and adaptive air defence systems that can effectively respond to any challenge in the modern combat environment.

Improvements in performance were achieved through the effective integration of air defense and electronic warfare systems, which increased the speed of adaptation, decision-making accuracy, and system flexibility. The introduction of the latest algorithms for data processing and the improvement of real-time methods have reduced the response time to threats, contributing to faster decision-making and the implementation of countermeasures. One of the main reasons for the improvements was the integration of more powerful processor units and the increased ability of the system to analyze large amounts of data under conditions of high information load intensity. Thanks to this, the system is able to identify threats faster and more accurately, adapt its parameters to new conditions, and adjust its actions in real time.

The nature of the observed phenomena is that with the introduction of electronic warfare, it became possible to reduce the impact of factors such as interference and misleading signals on air defense systems, allowing for more accurate detection of real threats and faster response to them. This has led to a reduction in adaptation time and improved accuracy in adjusting the system to new threat parameters. At the same time, thanks to the integration of electronic warfare, systems have become more flexible in their response to various types of threats, which has increased their overall effectiveness in changing and complex scenarios.

Challenges and Prospects for Integrated Air Defence and Electronic Warfare

An analysis of the joint capabilities of air defence radar and electronic warfare systems has revealed several key aspects that affect the effectiveness of protecting critical assets from air attacks. The results showed that synchronisation between these systems is critical to ensure a fast and accurate response to threats. Simulations of combat conditions have shown that proper coordination between air defence radar and electronic warfare systems significantly increases the effectiveness of neutralising air threats, reducing the time to detect and intercept a target. Marguerite Delcourt et al. (2021) confirmed that synchronisation of detection and electronic warfare systems is a key element in protecting critical assets. The integration of these systems creates a multi-layered defence, where each component complements the other, increasing the overall effectiveness of protection. Detecting threats at an early stage allows electronic warfare systems to respond quickly, minimising the risk of enemy penetration. The study by Sang Seo et al (2022) also showed that coordination between detection and electronic warfare systems is critical to the protection of strategic assets. Without proper coordination, gaps in protection arise, leaving facilities vulnerable. Effective interaction between the systems ensures a quick and accurate response to threats, making the most of their capabilities. It is worth noting that the effectiveness of synchronisation depends not only on the technical characteristics

of the systems but also on the ability of operators to quickly process the data and make appropriate decisions (Mussina et al., 2018). The introduction of modern information processing algorithms and automated control systems can significantly increase the efficiency of actions, which is critical in the context of protecting against fast-moving threats. Another important aspect is the regular updating and testing of systems to adapt to new types of threats, which allows maintaining a high level of preparedness for unforeseen situations (Semenenko et al., 2024).

One of the main conclusions of the study was that delays in data transmission or algorithmic inconsistencies harmed the overall effectiveness of the system. Although automated information exchange systems were able to reduce the time required to respond to threats, even minor delays in data transmission could lead to a decrease in missile guidance accuracy. This underscores the need to develop more resilient and faster data exchange systems that can ensure the instantaneous transfer of critical information between components of the defence network. Nikhil Kumar et al. (2024) concluded that delays in data transmission can significantly reduce the accuracy of threat neutralisation, especially during rapid attacks. Even a slight delay between detection systems and electronic warfare can lead to a delayed or incorrect response, increasing the risk of a successful attack on important facilities or troops. Richard Rudd-Orthner and Vito Pesare (2023) found that high-speed information exchange systems are critical to the protection of critical facilities. They must transmit data instantly with minimal delays, ensuring a quick and accurate response to threats. The use of advanced data communication technologies increases the efficiency of coordination and reduces the risk of errors (Shults et al., 2020). These results support the research cited above, as they demonstrate that even minor delays in data transmission can have a critical impact on the effectiveness of defence systems. The study showed that the speed of information exchange systems is directly related to the accuracy and efficiency of threat neutralisation. This underscores the importance of implementing advanced technologies to minimise delays and ensure reliable protection of facilities, which is a key factor in today's cyber and electronic warfare environment.

The rapid exchange of information between the detection and electronic warfare systems also proved to be an important factor in improving efficiency. The results showed that automating this process significantly reduced the likelihood of errors and increased the accuracy of the data supplied to the missile guidance system. Practical tests with real data have shown that the rapid exchange of information provides greater flexibility in responding to threats, especially in conditions of high information load and rapid changes in the situation on the battlefield. Oleg Sova et al. (2021) also found that rapid information exchange between detection and electronic warfare systems is key to effective defence. Instant data transfer ensures timely detection of threats and rapid response to them, increasing the overall effectiveness of defence and reducing the likelihood of errors. In turn, Nicholas R. Gans and John G. Rogers

III (2021) concluded that automation of data exchange minimises the human factor and reduces the risk of errors in decision-making. Automated systems can process large amounts of data in real-time, which allows them to quickly adapt to changing combat conditions and increase the effectiveness of defence (Apakhayev et al., 2018). These findings are consistent with the arguments presented in the previous section, as they confirm the importance of rapid and automated information exchange between detection and electronic warfare systems to ensure effective protection. As noted earlier, even minor delays or errors can have a critical impact on the outcome, making automated solutions particularly valuable in a combat environment. Thus, the integration of fast and reliable data exchange systems is not just desirable, but a prerequisite for the successful completion of defence tasks.

The real-time adaptability of systems was another important aspect of the study. Simulations showed that systems capable of automatically adjusting their parameters depending on the type of threat had significantly better performance in difficult combat conditions. Adaptability allowed electronic warfare systems to more effectively counter new types of threats arising during attacks, which in turn increased the overall level of protection of important facilities. Sangjun Kim et al. (2021) also conducted a study that confirmed that the real-time adaptability of detection and electronic warfare systems increases their effectiveness, allowing them to respond instantly to changes in attack tactics and new enemy technologies. This ensures a constant level of protection and reduces the risk of a successful breach. Serhii Lysenko et al. (2024) also found that the adaptation of systems to new types of threats is critical for reliable protection. Systems that can quickly update their strategies and algorithms are more effective in countering modern challenges, reducing the likelihood of the enemy exploiting weaknesses in the protection of facilities. Comparing the data obtained during the research, it can be argued that the adaptability of detection and electronic warfare systems is a key factor in their effectiveness. The results show that systems capable of responding quickly to new threats and changing their parameters in real time demonstrate significantly better performance in detecting and neutralising attacks. This confirms the importance of implementing adaptive algorithms and technologies to ensure reliable protection in a constantly changing combat environment.

However, despite the positive results, the study also revealed some challenges. For instance, integrating new technologies and ensuring their compatibility with existing systems proved to be a challenge (Raja et al., 2024). This underscores the need for further research and development in this area to ensure even greater effectiveness of joint operations between air defence radar and electronic warfare assets. Yuntao Wang et al. (2021) concluded that the integration of new technologies into existing defence systems faces challenges such as the high cost of modernisation and the difficulty of adapting new solutions to existing systems. Rapid technological

development can also lead to new solutions becoming obsolete before integration is complete. Elochukwu Ukwandu et al. (2022) found that ensuring system interoperability in the face of rapidly evolving threats is challenging. Technologies can quickly become obsolete due to new attack methods, making them difficult to update and integrate. This can lead to delays in the implementation of new solutions and a decrease in the overall effectiveness of defence systems. The study's findings make it clear that integrating new technologies into existing defence systems requires careful planning and consideration of potential challenges. Performance indicators can be significantly affected if new solutions are not adequately adapted to existing systems or if rapidly evolving threats are not considered. This underscores the need not only to innovate but also to continuously monitor and adapt systems to ensure they remain compatible and effective in a changing combat environment.

Overall, the results of the study showed that integration and coordination between air defence radar and electronic warfare assets are key to ensuring the effective protection of critical assets from air attacks. The further development and improvement of these systems, especially in terms of improving operational data exchange and real-time adaptability, is a promising area for enhancing defence capabilities in the face of modern threats.

Conclusions

The analysis of the joint actions of air defence radar and electronic warfare systems in the performance of tasks to protect important objects from air attacks has shown the importance of integrating these systems to improve defence effectiveness. The results of the study indicate that synchronisation of actions between detection and electronic warfare systems can significantly reduce the time required to respond to threats, improve missile guidance accuracy and increase the success of neutralising air attacks. Automation of information exchange between system components has significantly reduced data processing and decision-making time, which has increased the overall efficiency of the defence network.

The study also confirmed the importance of real-time adaptability of systems, which allows for a rapid response to changing combat conditions and new types of threats. Adaptive systems have demonstrated high flexibility and the ability to adjust their parameters to specific threats, which ensures stable defence effectiveness even in conditions of intense information load.

At the same time, the study revealed several challenges related to delays in data transmission and the need to further improve synchronisation algorithms. These challenges point to the need for further research to optimise the integration of detection and electronic warfare systems, as well as the introduction of new

technologies such as AI to improve the effectiveness of protecting critical assets from airborne attacks.

It is necessary to study the possibilities of using AI for automated coordination between air defence radar and electronic warfare assets to increase the effectiveness of protecting important facilities from modern air threats. One of the limitations of the study is that the modelling and analysis of joint actions of air defence radar and electronic warfare assets were carried out in simulation conditions that may not fully reflect the complexity and dynamics of real combat situations.

BIBLIOGRAPHY

[1] Al-Khawaja, A., Sadkhan, S.B., 2021. Intelligence and electronic warfare: challenges and future trends. In: Proceedings of the 7th International Conference on Contemporary Information Technology and Mathematics, 118-123. Mosul: Institute of Electrical and Electronics Engineers.

[2] Annenkov, A., Medvedskyi, Y., Demianenko, R., Adamenko, O., Soroka, V., 2023. Preliminary accuracy assessment of low-cost UAV data processing results. In: International Conference of Young Professionals "GeoTerrace 2023". Lviv: European Association of Geoscientists and Engineers.

[3] Apakhayev, N., Omarova, A.B., Kussainov, S., Nurahmetova, G.G., Buribayev, Y.A., Khamzina, Z.A., Kuandykov, B., Tlepina, S.V., Kala, N.S., 2018. Review on the outer space legislation: Problems and prospects. Statute Law Review, 39 (3).

[4] Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., Colajanni, M., 2022. Modeling realistic adversarial attacks against network intrusion detection systems. Digital Threats: Research and Practice, 3 (3).

[5] Astapenya, V., Zhdanova, Y., Shevchenko, S., Spasiteleva, S., Kryvoruchko, O., 2024. Conflict model of radio engineering systems under the threat of electronic warfare. In: Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems, 290-300. Kyiv: CEUR.

[6] Babak, V., Filonenko, S., Kalita, V., 2005. Acoustic emission under temperature tests of materials. Aviation, 9 (4).

[7] Basystiuk, O., Rybchak, Z., Betsa, D., 2024. Classification of military equipment based on computer vision methods. Bulletin of Cherkasy State Technological University, 29 (3).

[8] Biliuk, I., Shareyko, D., Fomenko, L., Savchenko, O., Havrylov, S., Maiboroda, O., 2022. Reduction of Numerical Arrays in Magnetometry Problems Calculations. In: Proceedings of the 2022 IEEE 4th International Conference on Modern Electrical and Energy System, MEES 2022. Kremenchuk: Institute of Electrical and Electronics Engineers.

[9] Biliuk, I., Shareyko, D., Savchenko, O., Havrylov, S., Mardziavko, V., Fomenko, L., 2023. Tracking System of a Micromanipulator Based on a Piezoelectric Motor. Proceedings of the 5th International Conference on Modern Electrical and Energy System, MEES 2023. Kremenchuk: Institute of Electrical and Electronics Engineers.

[10] Chamola, V., Kotesh, P., Agarwal, A., Gupta, N., Guizani, M., 2021. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad Hoc Networks, 111.

[11] Chen, Z., Yu, J., Dong, X., Ren, Z., 2021. Three-dimensional cooperative guidance strategy and guidance law for intercepting highly maneuvering target. Chinese Journal of Aeronautics, 34 (5).

[12] Cherniavska, T., Cherniavskyi, B., Sanikidze, T., Sharashenidze, A., Tortladze, M., Buleishvili, M., 2024. Optimization of medical logistics with bee colony algorithms in emergency, military conflict and post-war remediation settings. CEUR Workshop Proceedings, 3892.

[13] Cherniavskyi, B., 2025. Integration of Drones and Dio-Inspired Algorithms into Intelligent Transportation Logistics Systems for Post-war Remediation of Ukraine. Lecture Notes in Networks and Systems, 1336 LNNS.

[14] Chiper, F.L., Martian, A., Vladeanu, C., Marghescu, I., Craciunescu, R., Fratu, O., 2022. Drone detection and defense systems: Survey and a software-defined radio-based solution. Sensors, 22 (4).

[15] Dahan, E., Aviv, I., Diskin, T., 2025. Aerial Imagery Redefined: Next-Generation Approach to Object Classification. Information, 16 (2).

[16] Delcourt, M., Shereen, E., Dän, G., Le Boudec, J.Y., Paolone, M., 2021. Time-synchronization attack detection in unbalanced three-phase systems. IEEE Transactions on Smart Grid, 12 (5).

[17] Dolph, C., Lombaerts, T., Kawamura, E., Ippolito, C.A., Stepanyan, V., Iftekharuddin, K., Szatkowski, G., McSwain, R., Morris, C., Malekpour, M.R., Minwalla, C., 2022. Ground to air testing of a fused optical-radar aircraft detection and tracking system. AIAA SCITECH 2022 Forum. https://doi.org/10.2514/6.2022-0498.

[18] Gans, N.R., Rogers, J.G., 2021. Cooperative multirobot systems for military applications. Current Robotics Reports, 2.

[19] Gao, S., Su, S., Liangmushage, A., Wu, K., Chen, L., 2023. Research on low-cost missile borne landing point positioning device based on RDSS/SMS. In: Y. Jia, W. Zhang, Y. Fu, J. Wang (eds.), Chinese Intelligent Systems Conference (pp. 443-454). Singapore: Springer.

[20] Goecks, V.G., Waytowich, N., Asher, D.E., Jun Park, S., Mittrick, M., Richardson, J., Vindiola, M., Logie, A., Dennison, M., Trout, T., Narayanan, P., Kott, A., 2023. On games and simulators as a platform for development of artificial intelligence for command and control. The Journal of Defense Modeling and Simulation, 20 (4).

[21] Han, Q., Pang, B., Li, S., Li, N., Guo, P.S., Fan, C.L., Li, W.M., 2023. Evaluation method and optimization strategies of resilience for air & space defense system of systems based on kill network theory and improved self-information quantity. Defence Technology, 21.

[22] Kim, S., Eun, Y., Park, K.-J., 2021. Stealthy sensor attack detection and real-time performance recovery for resilient CPS. IEEE Transactions on Industrial Informatics, 17 (11).

[23] Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., Ukhach, V., 2024. Cyber security in Ukraine: Theoretical view and legal regulation. Law, Policy and Security, 2 (2).

[24] Kumar, N., Aryan, P., Raja, G.L., Muduli, U.R., 2024. Robust frequency-shifting based control amid false data injection attacks for interconnected power systems with communication delay. IEEE Transactions on Industry Applications, 60 (2).

[25] Lan, X., Chen, J., Zhao, Z., Zou, T., 2023. Cooperative guidance of multiple missiles: A hybrid coevolutionary approach. IEEE Transactions on Control Systems Technology, 32 (1).

[26] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., Tatarchenko, Y., 2024. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Economic Affairs, 69.

[27] Lyu, C., Zhan, R., 2022. Global analysis of active defense technologies for unmanned aerial vehicle. IEEE Aerospace and Electronic Systems Magazine, 37 (1).

[28] Mazahir, S., Ahmed, S., Alouini, M.S., 2021. A survey on joint communication-radar systems. Frontiers in Communications and Networks, 1.

[29] Moghaddam, B.M., Chhabra, R., 2021. On the guidance, navigation and control of in-orbit space robotic missions: A survey and prospective vision. Acta Astronautica, 184.

[30] Mussina, A., Ceccarelli, M., Balbayev, G., 2018. Neurorobotic investigation into the control of artificial eye movements. Mechanisms and Machine Science, 57.

[31] Nikolchuk, Yu., Lopatovska, O., 2023. Investment attractiveness of Ukraine: Trends, problems and solution key vectors. Innovation and Sustainability, 3 (1).

[32] Petrov, N., Sydykova, G., Dimitrova, K., Gospodinova, E., Tlegenov, A., Shegenbaeva, R., 2023. Study of the sustainability of functioning of electronic apparatus. AIP Conference Proceedings, 2889 (1).

[33] Potteiger, B., Dubey, A., Cai, F., Koutsoukos, X., Zhang, Z., 2022. Moving target defense for the security and resilience of mixed time and event triggered cyber-physical systems. Journal of Systems Architecture, 125.

[34] Raja, S., Mustafa, M.A., Ghadir, G.K., Al-Tmimi, H.M., Alani, Z.K., Rusho, M.A., Rajeswari, N., 2024. Unlocking the potential of polymer 3D printed electronics: Challenges and solutions. Applied Chemical Engineering, 7 (2).

[35] Reis, J., Cohen, Y., Melão, N., Costa, J., Jorge, D., 2021. High-tech defense industries: Developing autonomous intelligent systems. Applied Sciences, 11 (11).

[36] Rubino, G., Tomassi, G., Ciprini, L., Ali, S., Marignetti, F., 2022. Speed Sensorless Control based on Luenberger Observer for DC Motors. In: 2022 2nd International Conference on Sustainable Mobility Applications, Renewables and Technology, SMART 2022. Cassino: Institute of Electrical and Electronics Engineers.

[37] Rubino, L., Rubino, G., Conti, P., 2021. Design of a power system supervisory control with linear optimization for electrical load management in an aircraft on-board dc microgrid. Sustainability (Switzerland), 13 (15).

[38] Rudd-Orthner, R.N., Pesare, V., 2023. A naval combat management system (CMS) architecture to enable cognitive electronic warfare in platform protection. http://dx.doi.org/10.13140/RG.2.2.31979.00809.

[39] Semenenko, O., Nozdrachov, O., Chernyshova, I., Melnychenko, A., Momot, D., 2024. Innovative technologies to improve energy efficiency and security of military facilities. Machinery & Energetics, 15 (4).

[40] Seo, S., Han, S., & Kim, D., 2022. D-CEWS: DEVS-based cyber-electronic warfare M&S framework for enhanced communication effectiveness analysis in battlefield. Sensors, 22 (9).

[41] Sharma, M., Gupta, A.K., 2021. An algorithm for target detection, identification, tracking and estimation of motion for passive homing missile autopilot guidance. In: N. Marriwala, C.C. Tripathi, D. Kumar, S. Jain (eds.), Mobile Radio Communications and 5G Networks: Proceedings of MRCN 2020 (pp. 57-71). Singapore: Springer.

[42] Shults, R., Annenkov, A., 2023. BIM and UAV photogrammetry for spatial structures sustainability inventory. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives, 48 (5/W2-2023).

[43] Shults, R., Urazaliev, A., Annenkov, A., Nesterenko, O., Kucherenko, O., Kim, K., 2020. Different approaches to coordinate transformation parameters determination of nonhomogeneous coordinate systems. In: Environmental Engineering (Lithuania) (article number: enviro.2020.687). Vilnius: VGTU.

[44] Sova, O., Shyshatskyi, A., Salnikova, O., Zhuk, O., Trotsko, O., Hrokholskyi, Y., 2021. Development of a method for assessment and forecasting of the radio electronic environment. EUREKA: Physics and Engineering, 4.

[45] Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13 (3).

[46] Velastegui, N., Pavon, E., Jacome, H., Torres, F., Pico, M., 2022. Technological advances in military communications systems and equipment. Revista Minerva: Multidisciplinaria de Investigación Científica, 3 (8).

[47] Volkov, A., Brechka, M., Stadnichenko, V., Yaroshchuk, V., Cherkashyn, S., 2023. The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. Machinery & Energetics, 14 (4).

[48] Volkov, A., Yanenko, O., Kravchenko, S., 2019. Criteria for assessing the effectiveness of the organization of interaction during the air defense of troops. Digest of Scientific Works of Ivan Kozhedub Kharkiv National Air Force University, 3 (61).

[49] Wang, Y., Su, Z., Ni, J., Zhang, N., Shen, X., 2021. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. IEEE Communications Surveys & Tutorials, 24 (1).

[50] Xu, J., Huang, F., Wu, D., Cui, Y., Yan, Z., Zhang, K., 2021. Deep reinforcement learning based multi-AUVs cooperative decision-making for attack-defense confrontation missions. Ocean Engineering, 239.

[51] Yermolenko, R., Klekots, D., Gogota, O., 2024. Development of an algorithm for detecting commercial unmanned aerial vehicles using machine learning methods. Machinery & Energetics, 15 (2).

[52] Zaiets, K., Muravska, Y., Slipchenko, T., Kaniuka, V., Melnyk, I., 2024. The etymology of the concept "military conflict" as a determinant of political orientation. Law, Policy and Security, 2 (2).

[53] Zaverbnyj, A., 2024. Peculiarities of forming a cybersecurity management system for enterprises in wartime: Theoretical and applied aspect. Innovation and Sustainability, 4 (1).

[54] Zhang, C., Wang, L., Jiang, R., Hu, J., Xu, S., 2023. Radar jamming decision-making in cognitive electronic warfare: A review. IEEE Sensors Journal, 23 (11).