Machinery & Energetics
Vol. 14, No. 4. 2023

Journal homepage:
https://technicalscience.com.ua/en

UDC 355.358.4:624.01
DOI: 10.31548/machinery/4.2023.23

Andrii Volkov*

Head of the Department
Ivan Kozhedub Kharkiv National Air Force University
61045, 228 Klochkivska Str., Kharkiv, Ukraine
https://orcid.org/0000-0003-1566-9893

Mykhailo Brechka

PhD in Technical Sciences, Senior Lecturer
Ivan Kozhedub Kharkiv National Air Force University
61045, 228 Klochkivska Str., Kharkiv, Ukraine
https://orcid.org/0000-0003-1566-9893

Volodymyr Stadnichenko

Deputy Head of the Department
Ivan Kozhedub Kharkiv National Air Force University
61045, 228 Klochkivska Str., Kharkiv, Ukraine
https://orcid.org/0000-0002-1780-9215

Vitalii Yaroshchuk

Lecturer
Ivan Kozhedub Kharkiv National Air Force University
61045, 228 Klochkivska Str., Kharkiv, Ukraine
https://orcid.org/0000-0001-5318-5692

Serhii Cherkashyn

Lecturer
Ivan Kozhedub Kharkiv National Air Force University
61045, 228 Klochkivska Str., Kharkiv, Ukraine
https://orcid.org/0009-0002-6940-3863

The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means

Abstract. The relevance of the study is emphasised by the need to investigate and develop effective strategies for protecting critical state infrastructure in the context of the Russian-Ukrainian war of 2022. The purpose of this study is to evaluate the effectiveness of interaction between the means of physical and electronic influence in the context of protecting critical infrastructure facilities of the energy sector from air strikes. The object of research is the system of protection of critical facilities of the state's energy sector. Research methods included the use of system analysis, the development of strategies for determining the optimal locations of the means of physical influence, and the use of mathematical modelling. Research in the field of interaction and simultaneous use of physical and radio-electronic means included a theoretical analysis of abstract objects and their relationships. These objects were designed to create an idealised description and investigate possible scenarios, as well as to determine optimal actions in specific situations. This study examined in detail

Article's History: Received: 04.07.2023; Revised: 17.10.2023; Accepted: 22.11.2023.

Suggested Citation:
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), 23-32. doi: 10.31548/machinery/4.2023.23.

*Corresponding author

the possibilities of improving the effectiveness of protecting important energy facilities from air strikes through the use of combined strategies such as anti-aircraft fire and fire protection. Methods for determining the optimal locations of the means of physical influence were analysed, which allowed predicting expected results when using them together. It was developed evidence-based recommendations for the effective integration of these methods, which is an innovative approach to the problem. The means of physical influence included small arms, which were part of the armament of the Armed Forces, and interceptor drones. Electronic means of influence included technical means of radio frequency warfare and electromagnetic guns. The practical significance of this study lies in the fact that it presents specific strategies and technological solutions for comprehensive protection of critical infrastructure facilities from air strikes. This paper can serve as a basis for developing effective security and protection policies in countries and regions, helping to improve overall sustainability and security

Keywords: energy sector of the state; the Russian-Ukrainian war; means of physical influence; radio waves; air attack

INTRODUCTION

The need to investigate this topic is conditioned by modern geopolitical realities and the evolution of security threats. The results of terrorist attacks and examples of the use of drones to attack critical energy facilities indicate an increase in the vulnerability of states to new forms of aggression. The use of air strikes, in particular, through the use of unmanned aircraft, is becoming an effective tool for terrorist organisations and countries, and therefore, the study and development of strategies for the protection of critical facilities is an extremely urgent task for ensuring national and international security, and protecting the economic interests of states. A significant number of dangerous critical facilities in the world are located in most countries. The level of danger of a facility is set considering the percentage of the civilian population and the area of the territory that may become part of the zone of possible impact in the event of an accident at a facility. The results of terrorist attacks during 2019-2022 in the world and the course of the Russian-Ukrainian war show that the most dangerous objects today are facilities of the energy sector. In just nine months of 2022, more than 184 cruise missiles and more than 95 unmanned aerial vehicles were fired at Ukrainian cities where critical facilities of the state's energy sector are located, including more than 70 Iranian Shahed-136 kamikaze drones (Chronicle of the war..., 2022). According to estimates of the world's leading economists, the economic damage caused by these blows to the state amounts to more than 300 billion USD.

The problem of the study is that modern technologies, in particular the use of drones, open up new opportunities for attacks on critical facilities of the energy sector. The global experience of terrorist attacks and examples of air strikes during armed conflicts confirm that the energy sector is particularly vulnerable to such threats. However, providing comprehensive protection of critical facilities from air strikes is a complex task, as it requires a combination of means of physical and electronic influence, including new technologies in the field of unmanned aviation, and developing effective security management strategies.

According to H. Dementiiuk *et al.* (2023a), modern technologies allow effectively using methods of radio-electronic influence on energy sector facilities. The study does not detail the consideration of possible defence options during air strikes. I.Yu. Chaika & Ye.G. Tsokur (2022) emphasise the high vulnerability of critical facilities to air strikes. The effectiveness of possible protection measures against such threats is not investigated. According to V. Hurkovskyi *et al.* (2023), terrorist acts and examples of the use of drones in armed conflicts emphasise the need for a combination of means of physical and electronic influence to provide comprehensive protection. The analysis did not address specific aspects of the development or use of specific strategies for combining means of physical and electronic influence.

S. Korsunov *et al.* (2021) note that new opportunities for the use of unmanned aerial vehicles, in particular kamikaze unmanned aerial vehicles (UAVs), are highlighted. This paper does not address new security challenges. Research conducted by V. Berezutskyi & N. Berezutska (2022) emphasises the importance of developing security management strategies and determining optimal methods for protecting critical facilities from air strikes. The study does not analyse specific aspects of developing security management strategies and determining optimal methods for protecting critical facilities from air strikes. The paper by V. Dykha & V. Lukianova (2023) raises the question of possible economic losses as a result of attacks on energy facilities. This study does not provide a specific detailed analysis of possible measures to reduce economic losses as a result of attacks on energy facilities.

The purpose of this study is to determine the effectiveness of interaction between physical and radio-electronic means in the context of protecting critical infrastructure facilities of the energy sector from air strikes. Objectives of the study:

1. onduct an analysis of the interaction of means of physical and electronic influence to determine their compatibility.

2. Develop a methodology for determining the optimal location of means of physical influence when protecting critical facilities of the energy sector from air strikes.

3. Develop scientifically based recommendations for the effective use and interaction of physical and electronic means of influence.

MATERIALS AND METHODS

The object of this study is a comprehensive system for protecting facilities of critical importance that are part of the state's energy complex. After evaluation, it was found that this system includes various tools and technologies aimed at protecting these facilities from potential air strikes and other threats. The subject of this study is a detailed review and optimisation of the combined use of physical and electronic means of influence in the protection system. This included investigating the interaction of these tools, evaluating their effectiveness, and developing strategies for optimal use in the context of protecting critical energy facilities.

The use of the system analysis method identified key elements of the system and assessed their importance and relationships, which contributed to a deeper understanding of the problem and the development of effective protection strategies. The system analysis also allowed identifying possible risks and predicted their consequences, which is a key stage in the development of comprehensive strategies for protecting critical facilities. This method has created a theoretical and practical basis for further steps in implementing innovative solutions and developing practical protection strategies in the face of modern threats and challenges.

The method of mathematical modelling allowed considering various factors, such as geographical conditions, characteristics of means of influence, possible attack paths, and risk dynamics. By creating mathematical models, possible scenarios were evaluated and optimal parameters for the location of means of physical influence were determined to maximise the effectiveness of facility protection. The use of mathematical modelling contributed to a deep understanding of the impact of various factors on security and helped improve security strategies, making them more accurate and adapted to specific conditions. This is a key step in creating comprehensive protection strategies for critical facilities that take into account all possible scenarios and risks to ensure full protection.

The development of a methodology for choosing the location of means of physical influence included a detailed study of the topography and geographical features of the facility. This process took into account various factors, such as population density, environmental conditions, and possible attack routes. Special attention was paid to aerodynamic characteristics and altitude parameters in order to ensure the optimal location of means of physical influence to maximise their effectiveness in protecting facilities. In the course of the study, an algorithm for determining the optimal location of an anti-aircraft missile system when protecting a facility from an air strike was developed and improved, and key aspects of their optimal use in real-world protection conditions were identified.

RESULTS

Development of a methodology for determining the optimal location of physical protection for energy sector facilities against air strikes

To develop a methodology for determining the optimal location of means of physical influence (MPI) in the protection of critical facilities of the energy complex (CFEC) from air strikes, it is proposed to use an algorithm (Fig. 1), which provides for the sequential execution of a number of procedures and tasks. The initial data for calculating the distance between MPI (Block 1) are the types of air-to-air missiles (AAM) that can be applied to the protected facility, the geographical coordinates and spatial dimensions of the protected facility, the composition of MPI allocated for the protected facility, the highest level of efficiency in the use of MPI, and characteristics describing the effectiveness of the use of MPI. Source data is selected from pre-created data or generated during database preparation (Block 1).

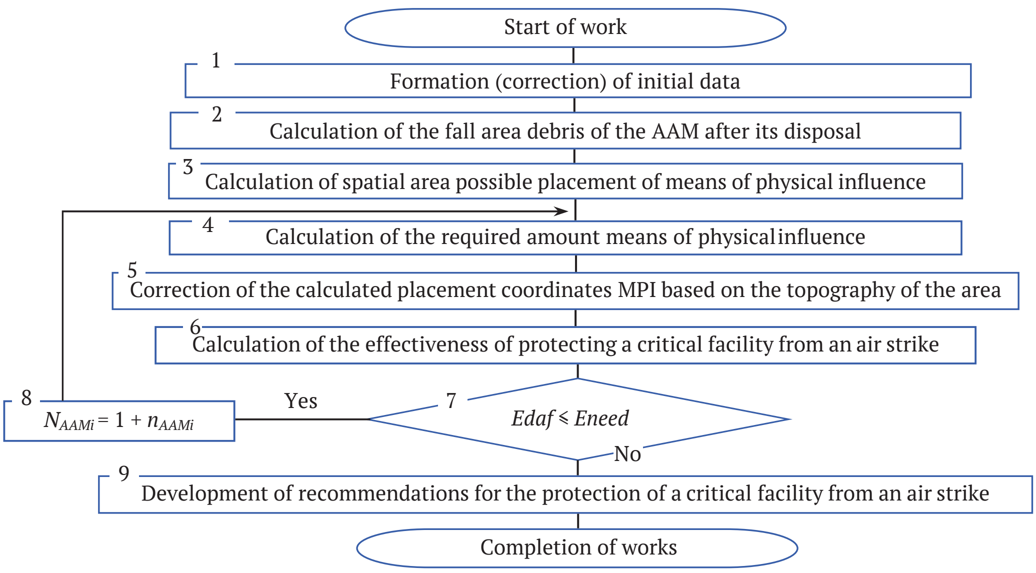

Figure 1. Algorithm for selecting the location of an anti-aircraft missile system when protecting a facility from an air strike
Source: compiled by the authors based on P. Hou *et al.* (2023)

In Block 2, the area of falling of fragments of an AAM after their neutralisation is calculated using the existing model (Park *et al.*, 2021). This calculation is key to determining the required distance by which locations should be removed from the perimeter of the protected facility. Analysis of the results of modelling the process of air defence system neutralisation during flight at different speeds and altitudes showed that the distance to the detection point should be within 1-2 km from the protected facility. Among the criteria that determine the effectiveness of MPI, the range of destruction of AAM from the protected facility, on which the task of their neutralisation is set, is of great importance. This range is determined by the specific means of physical influence, the flight altitude of the missile defence system, the time of detection and neutralisation, and the distance to which the defence zone extends from the facility. Setting the horizontal distance from the protected facility to its border, where tasks for the disposal of AAM are set, is carried out using the following equations:

$$d_{d.s.t} = d_{d.MPI} + V_{AAM}(t_{d.p.MPI} + t_{t.n}), \quad (1)$$

where: $d_{d.s.t}$ – horizontal distance from the protected facility to the task setting line, $d_{d.MPI}$ – distance of the MPI location from the protected facility, V_{AAM} – speed of air attack vehicle, $t_{d.p.MPI}$ – time of direct preparation of MPI for neutralisation of air attack vehicles, $t_{t.n}$ – time of neutralisation of air attack vehicles at the borders of the neutralisation zone.

Block 3 defines the area where the device can be placed for physical influence. Given the requirements for avoiding debris entering the protected facility, it is recommended to dispose of debris at an average distance of 2 km or more from the protected facility (depending on the type of debris). To do this, the location of anti-aircraft installations should be removed from the territory of the protected facility at a distance of 1 km or more. Increasing the distance of the MPI location increases the probability of saving the protected facility. On the other hand, the more remote the MPI is from the protected facility, the more tools need to be used for effective protection. It is noted that in practice there is a limited number of available tools (Kumar *et al.*, 2022). Therefore, it is recommended to determine the location of means of physical influence as close to the protected facility as possible, considering their characteristics and the number of MPI intended to protect this facility.

After determining the distance required for the location of the anti-aircraft system outside the protected facility, the required number of protection equipment is calculated in Block 4. The next step is to use the algorithm for correcting the calculated coordinates of the MPI location, based on the analysis of digital maps of the area (Block 5). If the terrain or natural obstacles affect the location of the MPI, its position can be adjusted. A programme is activated that reproduces the MPI on an electronic map in accordance with the proposed provision (Kasraei *et al.*, 2021). For a more detailed and high-quality assessment of the MPI location, Block 6 implements an algorithm for assessing the degree of protection of facility from physical influence. The assessment of the degree of security of the facility is presented in the form of a table with calculations, which reflects the coefficients of neutralisation zones and the load coefficients MPI. Based on this information (blocks 7-9), MPI location issues are resolved. Regarding the placement of electronic means of influence, it is advisable to note the definition of such places where they can operate without interfering with the operation of MPI. This is, for example, considering the norms of frequency-territorial propagation, the corresponding distance between MPI and radio-electronic influence (REI) when they work together.

Determination of the effectiveness of protection of critical energy facilities from air strikes due to the combined use of means of physical and electronic influence

To assess the impact of interaction between the means of physical and radio-electronic influence on the effectiveness of their joint action, it is important to analyse the essence of the term "compatibility" and logically establish the relationship of this concept with the terms related to "interaction of physical and radio-electronic influence" (Dementiiuk *et al.*, 2023b).

The terminological system and its elements should have interdependence, unambiguity in military-scientific and general scientific disciplines, context-independent clarity, correlation with only one concept, brevity and lexicographic approach to term formation, flexibility for expansion, clarification and changes, and the possibility that the term becomes a designation of a broader concept. Considering these requirements for terminology and analysing the existing basic terms, the "zone of joint action of means of physical influence and means of electronic influence" refers to the area of their location and the airspace where the neutralisation and suppression of means of air attack is carried out.

Scientific challenges in the study of the combined effects of means physical and radio-electronic influence in the protected areas of critical energy facilities are diverse, and their solution may vary depending on the specific case. Number of possible options (n_{var}) depends on the quantity and type, and can be determined using coefficients that take these parameters into account:

$$n_{var} = (\mathrm{N}_{\mathrm{MPI}_i} + 1)(\mathrm{N}_{\mathrm{MPI}_j} + 1)(\mathrm{N}_{\mathrm{n.r.s}} + 1)(\mathrm{N}_{\mathrm{r.r.s}} + 1) \dots, \quad (2)$$

where: $\mathrm{N}_{\mathrm{MPI}_i}$ – number of means related to *i*-th type of physical influence, $\mathrm{N}_{\mathrm{MPI}_j}$ – number of physical means of influence of the *j*-th type, $\mathrm{N}_{\mathrm{n.r.s}}$ – number of radio interference stations that are in the noise state, $\mathrm{N}_{\mathrm{r.r.s}}$ – number of pulse response radio interference stations.

The composition and location of means of physical and electronic influence are closely related and interdependent. This interdependence is conditioned by methodological approaches to justifying the optimal number and order of placement of funds. This is conditioned by the fact that the effectiveness of a joint action depends both on its composition and on the order in which it is implemented ($d_{l.MPI}$) and means of electronic influence ($d_{l.REI}$) from the boundaries of the protected facility and mutual distances between the means of protection ($D_{MPI\text{-}REI}$). Consequently, there is a complex interdependence of the efficiency of interaction between MPI and REI, which can be expressed in the form of a functional dependence:

$$E = f\{N_{MPI}\}|_{N_{REI},\, d_{l.MPI},\, d_{l.REI},\, D_{MPIi},\, D_{REIi},\, D_{MPI-REI}} = \text{const}, \quad (3)$$

$$E = f\{N_{REI}\}|_{N_{REI},\, d_{l.MPI},\, d_{l.REI},\, D_{MPIi},\, D_{REIi},\, D_{MPI-REI}} = \text{const}. \quad (4)$$

The locations of systems are regulated by the requirements of the task, which means that the location of means of physical influence must correspond to the distance from the boundaries of the security facility, which guarantees the removal of the disposal zone abroad, from which the AAM task can be performed. To assess the impact of the maximum efficiency of using MPI and REI on the effectiveness of their joint operation, let us return to the essence of the term "compatibility". The result of the effectiveness of measures in the protection of critical facilities of the energy complex is an m-dimensional vector, including three main groups of components: the achieved (expected) effect (g), time expenditure (t), and resource expenditure (c). The result of the effectiveness of measures to protect critical energy facilities is (m) a measurable vector that includes three main components: the result obtained (g), time (t), and the cost of material or financial resources (c):

$$Y^m = [g^m, c^m, t^m], \quad (5)$$

where: Y^m – effectiveness of actions, m – factors and conditions that affect the effectiveness of events; g^m – received (or expected) useful result, c^m – resource costs, t^m – time spent.

The most appropriate target task for means of physical influence when protecting facilities from air strikes is a measured indicator – the number of saved air defence equipment compared to their total number that were used during the strike. As for the choice of indicators of the ratio of opposing forces, the most complete confrontation between MPI and AAM can reflect the ratio:

$$\sigma_i = \frac{K_{MPI_i neutmax}\left[1-\left(1-P_{prob.MPI_i neut}\right)^n\right] K_{e.inf.prov} N_{MPI_i}}{D_{lim.par.MPI_i zone}\, N_{AAM}} = \frac{K_{MPI_i c.p.} K_{e.inf.prov}}{N_{AAM}}, \quad (6)$$

where: $K_{MPI_i neutmax}$ – maximum number of MPI of *i*-th types that are simultaneously neutralised, $P_{prob.MPI_i neut}$ – probability of neutralisation of MPI of *i*-th type, n – amount of resources spent, $K_{e.inf.prov}$ – efficiency coefficient of information support, N_{MPI_i} – number of MPI of *i*-th type, $D_{lim.par.MPI_i zone}$ – limit parameter of the neutralisation zone of MPI of *i*-th type, N_{AAM} – number of military personnel involved in the attack on the security facility, $K_{MPI_i c.p}$ – combat potential ratio of MPI of *i*-th type.

$$K_{e.inf.prov} = \frac{K_{coef.f.p} K_{mask} \left(1+N_{\Sigma_{t.p}}\right) N_{\Sigma_{i.m}}}{t_{s.MPI}\,(1-t_{i.c})}, \quad (7)$$

where: $K_{coef.f.p}$ – coefficient of similarity of false placements with true ones, K_{mask} – facility masking coefficient, $N_{\Sigma_{t.p}}$ – total number of forces and means of protecting the facility of air strikes that carry out disinformation measures, $N_{\Sigma_{i.m}}$ – total number of intelligence tools that are part of the forces and means of protecting facilities from air strikes includes information flows that are involved in the process of collecting information, $t_{s.MPI}$ – time of MPI stay at the location, $t_{i.c.}$ – time to collect information.

Therefore, the process of neutralisation of air defence systems during CFEC protection from air strikes is considered probabilistic, and its main characteristics are the relationship of the forces of the parties (Dementiiuk *et al.*, 2023b). To assess the effectiveness of the use of electronic warfare equipment to protect critical facilities, the mathematical expectation of the number of airs attacking systems exposed to REI $M_{AAM\ sup.REI}$ is used:

$$M_{AAM\ sup.REI} = N_{AAM.sup} \Delta P_{i.p}, \quad (8)$$

where: $M_{AAM\ sup.REI}$ – number of air defence systems that have been subjected to electronic influence (suppression), $\Delta P_{i.p}$ – increase in the probability of preserving a facility equal to the probability of a conditionally neutralised automated control system, which is determined depending on the number of conditionally neutralised automated control systems and is calculated using the equation:

$$\Delta P_{i.p} = P^p_{p.rei} - P^o_{p.a.rei}, \quad (9)$$

where: $P^p_{p.rei}$ – probability of preserving protected facility in case of resistance to electronic means of influence (obstruction of them), $P^o_{p.a.rei}$ – probability of preserving the protected facility without taking measures to counteract the means of electronic influence.

For a situation where facility protection is performed, equation (9) can be rewritten as follows:

$$P_{REI} = 1 - e^{-N_{REI}\Delta P_{p.s.REI}/N_{AAM}}, \quad (10)$$

where: $P_{p.s.REI}$ – probability of preserving a critical facility only REI, N_{REI} – number of REI, N_{AAM} – number of AAM.

The analysis indicates that when evaluating the effectiveness of actions, only the ability of physical or radio/electronic exposure to a certain amount of air defence equipment to destroy the protected facility is considered (Sowers *et al.*, 2017). Thus, considering the above-mentioned disadvantage, it is proposed to formalise the dependence in such a way as to determine the effectiveness of interaction:

$$P_i = 1 - e^{-\left(\frac{M_{m.e.dest.MPI}}{N_{AAM}} + K_{comp.}\frac{M_{m.e.dest.REI}}{N_{AAM}} + K_{o.r.}\frac{M_{m.e.dest.low.alt}}{N_{AAM}}\right)}, \quad (11)$$

where: $M_{m.e.dest.MPI}$ – mathematical expectation of the number of destroyed AAM MPI, K_{comp} – MPI and REI compatibility ratio, $M_{m.e.dest.REI}$ – mathematical expectation of the number of AAM destroyed by REI, $K_{o.r}$ – opportunity realisation coefficient, $M_{m.e.dest.low.alt}$ – mathematical expectation of the number of destroyed air defence systems at low altitudes.

Therefore, it can be determined that to evaluate the effectiveness of joint actions of MPI and REI locations, generalised indicators are used in the form of mathematical expectations of the number of AAM air attack vehicles that are not able to perform their assigned tasks (P_i), and calculated by equation (11). Based on the value of this indicator, it is possible to estimate the expected results of MPI and REI actions, the level of AAM losses, and the degree to which they perform their task of hitting a critical energy facility. For the location of means of physical influence on the site, the method of directed selection of possible options for the composition of means within the existing structure was used, while MPI was placed at fixed distances from each other relative to the security facility. To apply this methodology, coefficients were used:

$$D_{MPI\text{-}REI\ min} = a \cdot J, \quad (12)$$

where: $D_{MPI\text{-}REI\ min}$ – minimum range of MPI and REI from the centre of the protected facility, at which their specified number is evenly distributed at J intervals, a – uniformity coefficient.

For the relative location of MPI and REI, their relationship and their location relative to the protected facility are taken into account using the appropriate ratios:

$$D_{MPI-REImin} = D_{det} \leqslant 0{,}65 D_{r.a}, \quad (13)$$

where: D_{det} – detection range, $D_{r.a}$ – minimum supply of ammunition.

$$D_{r.a} = V_{AAM} T_{am.d.AAM\ min} - \Delta + V_{AAM} T_{AAM\ dest}, \quad (14)$$

where: V_{AAM}VVV – AAM speed, km/min, $T_{am.d.AAMmin}$ – time of dropping ammunition from the air defence system, min, Δ – lag of weapons (ammunition) using air defence systems, km, $T_{AAM\ dest}$ – time of destruction of AAM.

For effective protection of the facility by means of electronic influence, it is important to place the REI at a certain distance , which should have less value , and at best be zero. However, limiting the reduction in the distance of the REI location is associated with the risk of hitting the defence facility when using homing weapons with REI radiation. The condition that sets the minimum and optimal values has the following form:

$$D_{REI} \geqslant D_{r.d.am} + d_{r.prot} + 3\sigma_{a.s.error}, \quad (15)$$

where: $D_{r.d.am}$ – radius of destruction of protected facility by ammunition, $d_{r.prot}$ – radius of protected facility, $\sigma_{a.s.error}$ – average square error of a homing weapon.

The problem of calculating the distance between the locations of anti-aircraft missiles when protecting a facility from air strikes is solved by selecting the locations of anti-aircraft missiles (Ivanets *et al.*, 2023). The results show that it is strategically important to pre-place physical and electronic warfare equipment throughout the protected area or in key areas. The simulation performed in this study allowed estimating the probability of holding a protected target in the event of an air attack by a standard anti-aircraft missile, such as cruise missiles or unmanned aerial vehicles, at different altitudes (Fig. 2).

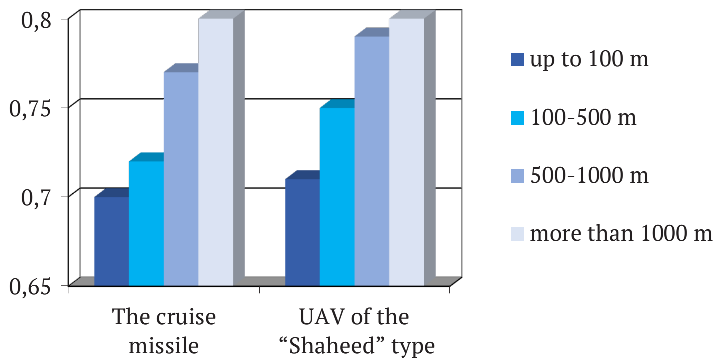

Figure 2. Diagram of the probability of preservation of critical facilities of the energy complex
Source: compiled by the authors

Analysis of the obtained data allows for the conclusion that the implementation of the proposed solutions can guarantee the safety of the protected facility during air strikes with a probability from 0.7 to 0.8 (Kopczewski *et al.*, 2023). Thus, the use of these recommendations will significantly increase the effectiveness of protecting both critical facilities and the civilian population, and territories from possible consequences of damage to energy facilities.

DISCUSSION

Protecting critical infrastructure facilities from air strikes is an extremely important task in the face of modern threats and conflicts. The ability to ensure effective protection of such facilities becomes strategically important not only for ensuring national security, but also for maintaining the stability and functioning of society. In the context of aviation threats, the modern development of unmanned aerial vehicles and cruise missiles creates new challenges for the protection of critical facilities. The combined use of various forces and means becomes a key aspect of the defence strategy. On the one hand, it is important to have effective means of physical influence, such as anti-aircraft systems, anti-aircraft missiles, and air defence systems that can provide active protection against aircraft and missiles. On the other hand, electronic means, such as early detection and prevention systems, can make important contributions to the prevention, detection, and neutralisation of threats. The effectiveness of the joint use of these forces and means is determined by their interaction and coordination. Research in the field of protecting critical infrastructure from air strikes can identify optimal strategies and technological solutions for this joint use. Solving these problems can serve as a basis for developing effective security and protection policies aimed at ensuring the stability and security of critical facilities in modern conditions of threats. This research can also contribute to the development of integrated protection strategies, taking into account the challenges of the modern military environment, and help improve security policies to ensure the sustainability of critical facilities.

Based on the results of recent study by M. Piekarski & K. Wojtasik (2022), protecting critical infrastructure from air threats in Poland is a high priority task in the context of modern security challenges. Poland, as a member of North Atlantic Treaty Organization (NATO) and the European Union (EU), faces a variety of potential threats, among which air attacks can be particularly serious. Given the country's geopolitical position, the importance of its economic infrastructure and energy facilities, effective protection becomes a key component of national security. Poland can use state-of-the-art technologies and strategies to ensure the protection of critical facilities. The development and improvement of early detection systems, air defences, and modern technical solutions for neutralising air threats can contribute to the creation of a reliable security system. The ability to integrate various means of physical and electronic influence, optimise their use and ensure coordination in activities is of great importance. Ukraine may also consider cooperation with other countries and international organisations to share experience and develop joint strategies in the field of critical infrastructure protection. This approach will ensure not only national, but also collective security in the face of increasing threats in the modern world.

Referring to the definition of T. Loveček *et al.* (2021), modelling and simulation are important tools for improving the protection of critical infrastructure and ensuring the sustainability of the basic needs of citizens. These approaches provide an opportunity to address complex challenges and identify optimal strategies for responding to possible threats. By creating mathematical models of vulnerabilities and scenarios of possible attacks, it is possible to effectively analyse the system and develop preventive measures. Simulations, in turn, allow virtually reproducing different situations and test the effectiveness of different protection strategies. These tools can be used to train personnel, analyse the reality of the security system, and improve infrastructure. Further development of simulation and simulation technologies can significantly improve preparedness and response to new threats, providing reliable protection for both critical infrastructure and the basic needs of citizens in today's unpredictable environment.

A.B. Daricili & S. Çelik (2022) determined that cybersecurity of critical infrastructure is a top priority in ensuring the sustainability of society in the face of an increasing number of cyber threats. Critical infrastructure, such as energy facilities, transportation systems, and communications, is being targeted by attempted cyber-attacks that can have serious consequences for national security. It is important to identify and implement measures to prevent cyber threats using advanced technologies and strategies. The development of effective systems for detecting and responding to cyber-attacks, and training personnel in the field of cybersecurity plays a key role in ensuring the integrity and operability of critical infrastructure. The analysis of the results and conclusions shows the relevance of using artificial intelligence and machine learning to predict and prevent cyber threats in the field of cybersecurity of critical infrastructure. Strengthening cooperation between government agencies, the private sector, and cybersecurity experts is becoming an important prerequisite for successfully countering cyber threats in critical infrastructure.

Researcher M. Böröcz (2021) determined that the policy of protecting critical infrastructure in the European Union is a key element of the strategy for ensuring national security and sustainability. This policy is developed and implemented to prevent and counter threats that may affect important sectors such as energy, transport, and telecommunications. One of the key initiatives is the creation of the European Union Agency for Cybersecurity (ENISA), which acts as a cybersecurity coordinator and consultant for EU member states. The centre promotes the exchange of information, provides recommendations and develops strategies to improve the protection of critical infrastructures in Europe. It can be agreed that considerable attention is also paid to the development of cyber defence standards and regulations that take into account the specifics of different critical infrastructure sectors. The introduction of innovative technologies such as artificial intelligence and blockchain into security systems is also becoming an important stage in the EU's critical infrastructure protection strategy.

As noted by Ł. Roman & K. Cygańczuk (2022), the legal dimension of protecting critical infrastructure is an important component of a national and international security strategy. Many countries are actively developing and improving legal frameworks for the effective protection of facilities of strategic importance for national security and sustainability. In most cases, these laws and regulations define the list of critical facilities, establish requirements for their protection, and also provide for liability for violation of these requirements. They can also define incident response procedures and interactions between public and private actors in protecting critical infrastructure. The findings of researchers confirm the results obtained. It is important to keep in mind that such a legal framework should be flexible and consider the rapid development of technologies and changing threats. Ensuring the effectiveness of these legal mechanisms requires constant updating and adaptation to new challenges, in particular, in the field of cybersecurity.

R. Cantelmi *et al.* (2021) showed by their work that in the context of the sustainability of critical infrastructure, the key element is the use of qualitative research approaches for comprehensive analysis and the development of effective protection strategies. One of these approaches – a system analysis method that allows considering a critical infrastructure as a complex system, considering the relationships and dependencies between its components. Researchers also actively use mathematical modelling to analyse the vulnerability and effectiveness of sustainability measures. This allows conducting scenario and strategic analyses, identifying weaknesses, and developing optimal protection methods. Modelling is also used to simulate a variety of scenarios, including natural disasters and cyber-attacks, which helps improve response and recovery strategies. However, it is important to note that the application of qualitative research methods also includes the analysis of modern technologies, considering socio-economic aspects and interaction between security actors. This approach allows viewing critical infrastructure in its full context, providing more effective sustainability and security management.

CONCLUSIONS

The list of critical energy sector targets for air strikes can be diverse and include important government facilities that require reliable protection from air strikes. Such facilities may include power plants, substations, gas pipelines, and infrastructure that is important for the normal functioning of the country and its economy. According to the above method, the means of physical and electronic influence are located at a certain distance from security facilities in order to prevent unmanned aerial vehicles and cruise missiles from entering the zone of critical energy facilities.

It is proposed to use physical means to protect critical energy facilities from air attacks, included in the integrated model for evaluating the effectiveness of using these means, provide an opportunity to confidently assert that their use in protecting critical energy facilities from air strikes will ensure its safety with a probability from 0.7 to 0.8. To assess the effectiveness of interaction between physical and electronic means, it is a generalised indicator in the form of mathematical expectation of the number of missiles that have not completed their mission, and is determined in relative terms. By the value of this indicator, it is possible to estimate the expected results of interaction between physical and electronic means of influence, the level of losses from air attack means and the degree of their performance of tasks.

The research shows the expediency of taking measures to improve the effectiveness of protecting critical facilities of the state's energy complex from air strikes due to the joint use of various forces and means, which is conditioned by the need to ensure the survival of the state, preserve th e environmental situation in the region of the location of a particular critical facility due to catastrophic consequences in case of damage.

It is advisable to further investigate the mechanisms of interaction and integration of innovative technologies in critical infrastructure protection systems to ensure the sustainability and effectiveness of countering modern aviation threats.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Berezutskyi, V., & Berezutska, N. (2022). Analysis of life protection of the population of cities and settlements during the war. *Science and Technology Today. Technics Series*, 8(8), 51-64. doi: 10.52058/2786-6025-2022-8(8)-51-64.

[2] Böröcz, M. (2021). Critical infrastructure protection policy in the EU. *Strategic Impact*, 3(80), 46-61. doi: 10.53477/1841-5784-21-15.

[3] Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 41(3), 341-376. doi: 10.1007/s10669-020-09795-8.

[4] Chaika, I.Yu., & Tsokur, Ye.G. (2022). The phenomenon of hybrid genocide in the conditions of the Russian-Ukrainian war of 2014-2022. *Political Life*, 4, 45-54. doi: 10.31558/2519-2949.2022.4.6.

[5] Chronicle of the war: A full-scale invasion of Ukraine. (2022). *Intent*. Retrieved from: https://intent.press/publications/politics/2022/hronika-vtorgnennya-rosiya-zatverdila-vvedennya-vijsk-na-shid-ukrayini/.

[6] Daricili, A.B., & Çelik, S. (2022). National Security 2.0: The cyber security of critical infrastructure. *PERCEPTIONS: Journal of International Affairs*, 26(2), 259-276.

[7] Dementiiuk, H., Basarab, O., Horbachov, K., Yanenko, O., Volkov, A., Tokar, O., & Iasechko, M. (2023a). Development of the principles of protecting critical infrastructure facilities against the destructive impact of cruise missiles with radio-location correlation extreme guiding algorithms based on the application of an electromagnetic screen. *Scandinavian Journal of Information Systems*, 35(1), 185-193.

[8] Dementiiuk, H., Iasechko, M., Kolesnichenko, S., Polianskyi, K., Basarab, O., Horbachov, K., Yanenko, O., & Zaitsev, I. (2023b). Princes and requirements for the protection of civilian infrastructure from the devastating effects of air attack. *Revista De Gestão Social E Ambiental*, 17(4), article number e03421. doi: 10.24857/rgsa.v17n4-028.

[9] Dykha, V., & Lukianova, V. (2023). Energy market risks: Essence of definition and characteristics. *Modeling the Development of the Economic Systems*, 1, 28-36. doi: 10.31891/mdes/2023-7-4.

[10] Hou, P., Pei, Y., Ge, Y., & Zhu, M. (2023). Terminal attitude selection method of missile attack aircraft. *Chinese Journal of Aeronautics*. doi: 10.1016/j.cja.2023.09.019.

[11] Hurkovskyi, V., Kozak, I., & Dmitruk, S. (2023). Technological and communication challenges of SBU and AFU interaction during armed aggression: Seeking innovative solutions. *Scientific Perspectives*, 38(8), 112-121. doi: 10.52058/2708-7530-2023-8(38)-112-121.

[12] Ivanets, M., Kutsenko, V., Artikula, A., Shinkarenko, O., & Yachna, I. (2023). Management algorithm for the comprehensive system of testing samples of anti-aircraft missile systems. *Testing and Certification*, 1(1), 17-24. doi: 10.37701/ts.01.2023.02.

[13] Kasraei, B., Heung, B., Saurette, D.D., Schmidt, M.G., Bulmer, C.E., & Bethel, W. (2021). Quantile regression as a generic approach for estimating uncertainty of digital soil maps produced from machine-learning. *Environmental Modelling & Software*, 144, article number 105139. doi: 10.1016/j.envsoft.2021.105139.

[14] Kopczewski, M., Grobelny, Z., & Świętochowski, N. (2023). Defense and deterrence as the foundation of the a2/ad system in smart city air defense. *Safety & Defense*, 9(1), 14-23. doi: 10.37105/sd.198.

[15] Korsunov, S., Volkov, A., Oboronov, M., Oriekhov, S., Gurtovenko, V., & Fedchenko, S. (2021). Transformation of unmanned aviation tasks from its creation to application in modern military conflicts. *Science and Technology of the Air Force of Ukraine*, 3(44), 66-81. doi: 10.30748/nitps.2021.44.08.

[16] Kumar, A., Yadav, A.S., Gill, S.S., Pervaiz, H., Ni, Q., & Buyya, R. (2022). A secure drone-to-drone communication and software defined drone network-enabled traffic monitoring system. *Simulation Modelling Practice and Theory*, 120, article number 102621. doi: 10.1016/j.simpat.2022.102621.

[17] Loveček, T., Straková, L., & Kampová, K. (2021). Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens. *Sustainability*, 13(11), article number 5898. doi: 10.3390/su13115898.

[18] Park, S., Kim, H.T., Lee, S., Joo, H., & Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access*, 9, 42635-42659. doi: 10.1109/ACCESS.2021.3065926.

[19] Piekarski, M., & Wojtasik, K. (2022). Protection of Polish critical infrastructure (CI) against air threats. *Security and Defence Quarterly*, 39(3), 76-87. doi: 10.35467/sdq/147676.

[20] Roman, Ł., & Cygańczuk, K. (2022). Legal dimension of the protection of critical infrastructure – Selected aspects. *Safety & Fire Technology*, 59(1), 166-181.

[21] Sowers, J.L., Weinthal, E., & Zawahri, N. (2017). Targeting environmental infrastructures, international law, and civilians in the new Middle Eastern wars. *Security Dialogue*, 48(5), 410-430.

Андрій Федорович Волков
Завідувач кафедри
Харківський національний університет Повітряних Сил імені І. Кожедуба
61045, вул. Клочківська, 228, м. Харків, Україна
https://orcid.org/0000-0003-1566-9893

Михайло Михайлович Бречка
Кандидат технічних наук, старший викладач
Харківський національний університет Повітряних Сил імені І. Кожедуба
61045, вул. Клочківська, 228, м. Харків, Україна
https://orcid.org/0000-0002-0291-9665

Володимир Григорович Стадніченко
Заступник завідувача кафедри
Харківський національний університет Повітряних Сил імені І. Кожедуба
61045, вул. Клочківська, 228, м. Харків, Україна
https://orcid.org/0000-0002-1780-9215

Віталій Володимирович Ярощук
Викладач
Харківський національний університет Повітряних Сил імені І. Кожедуба
61045, вул. Клочківська, 228, м. Харків, Україна
https://orcid.org/0000-0001-5318-5692

Сергій Володимирович Черкашин
Викладач
Харківський національний університет Повітряних Сил імені І. Кожедуба
61045, вул. Клочківська, 228, м. Харків, Україна
https://orcid.org/0009-0002-6940-3863

Захист об'єктів критичної інфраструктури від повітряних ударів завдяки сумісному застосуванню різних сил і засобів

Анотація. Актуальність дослідження підкреслюється необхідністю вивчення та розробки ефективних стратегій захисту критично важливих об'єктів інфраструктури держави, в контексті російсько-української війни 2022 року. Метою даного дослідження є оцінка ефективності взаємодії між фізичними та радіоелектронними засобами впливу у контексті захисту об'єктів критичної інфраструктури енергетичного комплексу від атак повітряних ударів. Об'єктом дослідження є система захисту критично важливих об'єктів енергетичного комплексу держави. Дослідницькі методи включали в себе використання системного аналізу, розробку стратегій для визначення оптимальних місць розташування засобів фізичного впливу та використання математичного моделювання. Дослідження в області взаємодії та одночасного використання фізичних та радіоелектронних засобів включало теоретичний аналіз абстрактних об'єктів та їх взаємозв'язків. Ці об'єкти конструювалися для створення ідеалізованого опису та вивчення можливих сценаріїв, а також для визначення оптимальних дій у конкретних ситуаціях. У цьому дослідженні детально розглядалися можливості підвищення ефективності захисту важливих об'єктів енергетичного комплексу від авіаударів за допомогою використання комбінованих стратегій, таких як зенітний вогонь та протипожежний захист. Аналізувалися методи визначення оптимальних місць розташування засобів фізичного впливу, що дозволяли передбачати очікувані результати при їхньому спільному використанні. Розроблено науково-обґрунтовані рекомендації з ефективного інтегрування цих методів, що є новаторським підходом до проблеми. Засоби фізичного впливу включали стрілецьку зброю, яка становила частину озброєння Збройних Сил та інших правоохоронних органів, а також безпілотники-перехоплювачі. Засоби радіоелектронного впливу включали в себе технічні засоби радіочастотної боротьби та електромагнітні гармати. Практичне значення цієї роботи полягає в тому, що вона представляє конкретні стратегії та технологічні рішення для комплексного захисту об'єктів критичної інфраструктури від авіаударів. Це дослідження може служити основою для розробки ефективних політик безпеки та захисту в країнах та регіонах, сприяючи підвищенню загального рівня стійкості та безпеки

Ключові слова: енергетичний комплекс держави; російсько-українська війна; засоби фізичного впливу; радіохвилі; повітряний напад