UDC 005.963.1:629.7.-027.3 **doi: 10.32620/aktt.2025.4.11**

Oleg FEDOROVICH[1], Oleg ZAMIRETS[2], Andrei POPOV[1], Oleksii HUBKA[1], Yuliia MALIEIEVA[1], Andrii RYBKA[1]

[1] ***National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine***
[2] ***State Enterprise Scientific Research Technological Institute of Instrument Engineering (SE SRTIIE), Kharkiv, Ukraine***

MODELING OF THREATS TO CRITICAL INFRASTRUCTURE OBJECTS FOR THE CREATION OF DEFENSES AGAINST SWARM ATTACKS BY STRIKE DRONES

Modern technologies used in hybrid warfare allow the enemy to perform large-scale attacks on critical infrastructure (e.g., transport, energy, industrial enterprises, etc.), which affects the country's economy. The use of unmanned aerial vehicles (UAVs) by the enemy in the form of swarms of strike drones has significantly increased the risk of damage to critical infrastructure objects (CIOs), which degrade over time and have dangerous vulnerabilities. Therefore, modeling defensive measures to protect CIOs from massive enemy air attacks is important. ***The subject*** *of this study is the creation of mathematical and simulation models for planning preventive measures in CIO defense. This research* ***aims*** *to create a set of models that can be used to analyze and identify threatening vulnerabilities of critical infrastructure objects triggered by wave attacks of enemy strike drones and to plan appropriate preventive defensive actions under limited capabilities.* ***The tasks*** *to be solved are as follows: conduct a systematic analysis of the sequence of actions for planning CIO defense; identify the most threatening vulnerabilities of CIOs that could be attacked by the enemy; make a rational distribution of defense capabilities to protect CIO, taking into account the enemy's capabilities to create strike capabilities using combat drones; and develop a multi-agent simulation model to analyze possible CIO damage from massive attacks by strike drones.* ***Mathematical methods and models*** *used: system analysis of preventive measures for CIO defense; qualitative assessment of CIO indicators to identify threatening vulnerabilities; lexicographic ordering of options to identify a set of relevant CIOs that need to be defended; integer (Boolean) optimization for the rational distribution of limited defense capabilities across locations of threatening CIO vulnerabilities; multi-agent simulation modeling of enemy wave drone attacks to analyze CIO damage. The following* ***results*** *were achieved: a logical sequence of preventive measures for CIO defense has been formed; a set of threatening vulnerabilities in CIO has been identified; the strike potential and capabilities of the enemy in terms of CIO vulnerability have been analyzed; the necessary defense potential for protecting CIO has been formed; various scenarios of strike drone attacks and possible CIO damage have been modeled; and a rational distribution of anti-drone means has been carried out to reduce the risks of CIO damage.* ***Conclusions****: the proposed set of models allows us to justify the logical sequence of preventive measures to defend CIOs against massive wave attacks by enemy strike drones. This will ensure the effective use of existing anti-drone defense measures against enemy attacks, even under conditions of limited capabilities. The scientific novelty of the proposed approach lies in the justification of protective measures for critical infrastructure against massive wave attacks by enemy strike drones based on a set of original and new mathematical and simulation models.*

.

Keywords: *critical infrastructure vulnerabilities; preventive measures for defense; wave attacks by strike drones; qualitative assessment of vulnerabilities; lexicographic ordering of options; optimization of defense potential distribution; multi-agent modeling of wave drone attacks.*

1. Introduction

The widespread use of new technological warfare tools, such as UAVs, by the enemy has led to the need to create reliable defenses for critical infrastructure objects (CIO) (transportation routes, logistics warehouses, energy facilities, industrial enterprises, etc.) against wave attacks by enemy strike drones [1, 2]. Improving the characteristics of combat drones (range and flight time, altitude, speed, combat load, etc.) requires an analysis of possible targets selected by the enemy [3, 4]. The set of objects that can be attacked by the enemy makes it necessary to take preventive decisions regarding the creation of defenses [5, 6]. However, limited possibilities for the use of defensive means lead to the search for threatening vulnerabilities, which will be used by the enemy as targets in the first place. Therefore, there is a complex task of analyzing possible vul-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

nerabilities that are critical for CIO when developing preventive measures for defense and preventing their destruction [7, 8]. After identifying threatening vulnerabilities, it is necessary to form a defense capability capable of ensuring protection and minimizing damage from aggressive enemy actions [9, 10]. To create a defense for vulnerable CIOs, it is necessary to analyze the enemy's potential strike capability in the form of a swarm of attacking drones (F") [11, 12]. Next, it is necessary to create an appropriate defensive capability (F') to protect CIOs, using existing anti-drone measures (air defense, electronic warfare, etc.), so that (F'≥F") [13, 14]. However, limited capabilities to allocate anti-drone measures (ADM) for defense have led to the need to identify the most threatening CIO vulnerabilities, which must be protected first [15, 16]. Taking into account the above, we can conclude that it is relevant to conduct research on the analysis of vulnerabilities that affect the damage to critical infrastructure objects in order to create the necessary defense.

1.1. Motivation

Planning defensive actions to protect critical objects, taking into account their vulnerabilities, from massive wave swarm attacks by enemy strike drones is a difficult task, as it is necessary to predict possible attacking actions as well as the enemy's ability to create strike potential (F">F') and select targets to be attacked. Preventive defense measures must be taken in advance to minimize the risk of CIO damage. To do this, it is necessary to create a set of anti-drone means using the possibility of allocating them. Therefore, it is important to identify threatening CIO vulnerabilities to assess the necessary defense potential for their protection.

1.2. State of the Art and problem statement

There are a number of problems that have arisen and are related to the protection of critical infrastructure from massive wave attacks by enemy strike drones. Some of them are being resolved, but there are new problems that require research. Let us consider some of the work in the areas listed below.

1. Formation of a set of critical infrastructure facilities that need to be protected from massive enemy attacks, given the limited capabilities for creating a full-fledged defense.

The authors of [17] provide a definition of critical infrastructure, which is used by governments to consolidate all resources necessary for the economic, financial, and social systems of a country. In the US, Presidential Policy Directive 21 (PPD-21) identifies 16 sectors of critical infrastructure. In Ukraine, the task of forming registers of critical infrastructure objects is being solved using a methodology based on relevant criteria that will determine whether a particular object is critical to the state [18]. The integration of ten criteria with the possibility of further expansion has been proposed, which is used to prioritize the protection of critical infrastructure facilities from attacks.

2. Identification of critical vulnerabilities of critical infrastructure facilities that affect their functioning.

The work [19] analyzes the vulnerability and risks of critical infrastructures. The structure of the vulnerability and risk analysis system is considered in connection with its application for the protection and resilience of critical infrastructures. It is argued that the complexity of these systems requires the integration of different modeling perspectives and new approaches to analysis. The authors of article [20] have developed a sustainable vulnerability model that measures and quantifies threshold vulnerability. The model reflects a system of measures for protection and resilience, requires input from experts in the subject area, and is deployed in a typical natural gas pipeline system, with data uncertainty taken into account through data aggregation and modeling.

3. Forecasting the enemy's capabilities to carry out a massive attack on multiple critical infrastructure objects.

Article [21] proposes a model of threats to critical infrastructure that takes into account the possible synergistic features of the integration of target threats and their hybrid nature; a method for determining enemy capabilities has been developed. A security assessment concept has been implemented that allows the formation of a unified threat database. The authors [22] address the tasks of assessing hostile situations, threats, and intentions, as well as forecasting these conditions for the future for decision-making purposes.

4. Assessment of the enemy's potential strike capability in the form of a swarm of strike drones that will be used in a wave attack on critical infrastructure facilities.

Article [23] proposes a methodological approach to assessing the combat potential of unmanned aerial vehicle systems (UAVS), their units, and formations, which takes into account the specific features of modern UAVS. The approach also takes into account combat conditions: the presence of false enemy targets and their camouflage; the presence of UAVs of different purposes in the group and the specifics of their joint use. Publication [24] highlights the task of assessing swarms of strike UAVs, which are divided into combat tasks and combat support (security) tasks. The main requirements for performance indicators are presented, and a general classification of indicators for the use of strike UAV swarms is proposed, with a conditional division into several groups.

5. Analysis of the possibilities for creating defenses for critical infrastructure facilities, taking into account their vulnerabilities.

In [25], a methodology for determining the importance of air defense facilities using factor analysis is proposed. The importance of facilities is adapted to the realities of the current situation, which is predicted and constantly changing. This ensures high-quality planning of air defense and assessment of its effectiveness in operations. The authors of study [26] consider the issue of comprehensive construction of a system for active protection of critical infrastructure facilities from air attack using several types of weapons. Based on the analysis of the enemy's use of various classes of missiles and Shahed-type strike UAVs, the use of engineering munitions is proposed as one of the means of destroying low-flying, slow-moving air targets.

6. The problem of the rational distribution of defense resources for the protection of critical infrastructure facilities under conditions of limited capabilities.

The work [27] considers the organizational and technical aspects of building an effective engineering protection system. According to the "fortress country" principle developed by the authors, three types of engineering protection of objects and stages of their gradual implementation are proposed. There is a study [28] aimed at improving the protection of critical infrastructure objects, which proposes the use of a wide range of short-range weapon systems and complexes. The issue of the location of protection systems directly in or near populated areas has been resolved, as has the rational use of weapons, ammunition, and other equipment and materials related to the functioning of facility protection systems.

7. Development of necessary preventive measures to protect critical infrastructure facilities while minimizing the risk of their destruction by massive enemy drone attacks.

Work [29] proposes a methodological framework for assessing the risk of drone intrusion into airports, adapted to the characteristics of drone attacks, airport characteristics, and current operations, as well as taking into account reasons related to both safety and security. The structure is based on a combination of model- and data-based approaches to: assess an airport's vulnerability index to measure its susceptibility to drone intrusion based on reference datasets; determine a set of event trees to assess the risks of various threat scenarios related to drone intrusion. The authors of article [30] implemented a decision support procedure for prioritizing threats to critical infrastructure, taking into account the degree of risk, probability, and potential damage from damage. The use of expert assessment methods makes it possible to study risks to critical infrastructure in conditions of a priori uncertainty, taking into account the probabilistic nature of military actions and the stochastic nature of missile and drone attacks.

This is not a complete list of problems, which continue to be supplemented by new ones in the context of modern hybrid warfare, indicating the relevance of conducting research to identify threatening vulnerabilities in critical infrastructure facilities for planning measures to defend them. This paper presents solutions to some of these pressing problems.

1.3. Objectives and methodology

There is a contradiction between the need to justify the protection of critical infrastructure from enemy strike drone missions and the imperfection and lack of methods, models, and information technologies that would allow fully conduct a systematic analysis of the existing vulnerabilities of critical infrastructure facilities to enemy strike drone air attacks, assess the possible level of damage, plan preventive measures for protection, and develop the necessary defense capabilities.

The aim of the study is to create a set of models that can be used to analyze and identify critical infrastructure vulnerabilities to enemy drone wave attacks and plan appropriate preventive defense actions under limited conditions.

In accordance with the stated aim, the following tasks must be solved:

1. Conduct a systematic analysis of the logistical sequence of actions for planning preventive measures to defend critical infrastructure facilities against wave attacks by enemy strike drones.

2. Analyze the vulnerabilities of critical infrastructure facilities and identify the most threatening ones.

3. Develop defensive capabilities in the form of anti-drone measures.

4. Develop a multi-agent model for analyzing possible damage to critical infrastructure facilities from enemy strike drone attack missions.

The article is structured as follows:

Section 2 is devoted to a systematic analysis of the planning of preventive measures for the defense of critical infrastructure facilities.

Section 3 contains an analysis and identification of the most threatening vulnerabilities of critical infrastructure facilities to possible damage from enemy drone attacks.

Section 4 is devoted to assessing the potential strike capability of the enemy in the form of combat drones and justifying the necessary defense capabilities for protecting critical infrastructure facilities under conditions of limited capabilities.

Section 5 is devoted to the creation of a multi-agent model for analyzing possible damage to critical infrastructure from enemy strike drone attacks.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Section 6 contains a discussion of the scientific results and their presentation in the form of a methodology that emphasizes the significance of the research for practical application.

Chapter 7 concludes the article by summarizing the conclusions and providing prospects for further research and the creation of applied information technology for planning defensive actions against enemy drone attacks.

2. System analysis of the logistics sequence of actions for planning preventive measures to defend critical infrastructure facilities from wave attacks by enemy strike drones

Critical infrastructure facilities are used by the enemy as targets because they have dual purposes (military and civilian). The enemy's offensive missions, using strike UAVs, are aimed at completely destroying CIO facilities that have vulnerabilities. Vulnerabilities arise from the deterioration of external conditions for CIO operation and the aging of individual components of the distributed system, leading to degradation and an increase in the number of vulnerabilities that can be exploited by external aggressive influences from enemy attacks. The enemy's preliminary actions before launching a massive attack with a swarm of strike drones are aimed at identifying, using reconnaissance, the vulnerable locations of CIO vulnerabilities in order to inflict maximum damage with minimum strike potential. Therefore, it is necessary for each CIO to analyze in advance the possible set of vulnerabilities in order to identify the most threatening ones. The identified CIO vulnerabilities require, first and foremost, protection against enemy strike drone attacks. Locations where threatening vulnerabilities are found must be protected using anti-drone measures (ADM) in the form of anti-aircraft, air defense, electronic warfare, etc. The existence of multiple CIOs that can be attacked by enemy strike drones, taking into account threatening vulnerabilities, necessitates the rational distribution of available ADM, given the limited possibilities for allocating them to protect all CIOs. The assessment of the enemy's potential strike capability (F''') is the basis for the distribution of ADM, taking into account the level of threat to CIO vulnerabilities, when creating defense capabilities (F') in the form of a set of ADM. It is necessary that $F' \geq F''$, which is not always possible. Thus, a logistical sequence of defensive measures arises, which must be investigated to create CIO protection with the presence of vulnerabilities:

analysis and identification of possible vulnerabilities → identification of the most threatening CIO vulnerabilities → prediction of possible wave attacks by enemy strike drones → assessment of the enemy's strike potential → assessment of the necessary defense potential for CIO protection (taking into account threatening vulnerabilities) → distribution of anti-drone means (available) for CIO protection → modeling of possible enemy damage to CIO after vulnerabilities are exploited.

To study the presented logistical sequence of actions for defending CIO from swarm attacks by enemy drones, it is necessary to:

1. Develop a model for identifying CIO vulnerabilities.
2. Use military experts' assessments of the CIO that will be attacked by the enemy first.
3. Develop indicators for assessing and identifying critical CIO vulnerabilities.
4. Develop an optimization model for the rational formation of defense capabilities in the form of ADM for CIO protection, taking into account the enemy's strike potential.
5. Simulate, in time, a massive attack by enemy strike drones to analyze possible damage to CIO.

The presented list of logistical actions and necessary models for research can be supplemented with new ones as innovations appear, both operational-tactical and technological, in modern hybrid warfare, using wave swarm attacks by the enemy.

Thus, it can be argued that there is a need to develop a set of models that will allow researching and predicting the success of preventive measures to protect critical infrastructure, taking into account their vulnerabilities to enemy air attacks using strike drones.

3. Analysis of critical infrastructure objects' vulnerabilities, with identification of the most threatening ones

Over time, critical infrastructure gets old, which can lead to vulnerabilities that enemies can use to attack with strike drones.

So, it's important to find CIO vulnerabilities and figure out where they are so enemies can't use them to attack.

The formation of vulnerabilities in CIOs is associated with the manifestation of the following factors:

- physical condition of the CIO;
- long period of CIO operation, with possible violation of service life;
- presence of CIO components that frequently fail and require repair (emergency) actions;
- violation of scheduled maintenance deadlines;
- violation of CIO operating conditions;
- lack of qualified personnel to maintain the CIO;

- the impact of aggressive external factors on the functioning of the CIO.

Vulnerabilities that arise and deepen over time have specific locations in distributed critical infrastructure systems that are potential targets for enemy attacks, taking into account waves of strike drones.

This leads to the exploitation of vulnerabilities and the disruption of CIO functioning and losses. To analyze vulnerabilities, it is necessary to develop indicators for their assessment. In this paper, we will use the following indicators to assess the contagiousness of CIO vulnerabilities:

1. Impact of the exploited vulnerability on the overall state of the CIO – (L1).

2. Number of personnel who may be affected by the exploitation of a vulnerability (enemy attack) – (L2).

3. Size of damage caused by enemy drone attacks on CIO vulnerability locations – (L3).

4. Risk of man-made impact of the triggered vulnerability on the external environment and people (possible man-made disaster) – (L4).

5. Level of protection of the CIO location (taking into account the category of the object) – (L5).

This is not a complete list of indicators, which may vary depending on the characteristics of the CIO and possible enemy attacks using strike drones.

The simplest use of the presented indicators for vulnerability impact analysis will be carried out by experts based on qualitative assessment.

Therefore, to present the values of the indicators in a qualitative form, we will use the linguistic variable y_{ik}, where the index "i" is related to the i-th vulnerability of the CIO, and "k" refers to the k-th indicator:

$$y_{ik} = \begin{cases} \text{G – level of k-th indicator is "green"} \\ \quad \text{in relation to i-th vulnerability;} \\ \text{O – level of k-th indicator is "orange"} \\ \quad \text{in relation to i-th vulnerability;} \\ \text{R – level of k-th indicator is "red"} \\ \quad \text{in relation to i-th vulnerability.} \end{cases} \quad (1)$$

Using the values of the linguistic variable y_{ik}, for each vulnerability, we can form a set of indicator values (L1, L2, L3, L4, L5) that characterizes the threat level of the i-th vulnerability. At the same time, it is necessary to establish in advance the priority of indicators depending on the characteristics of the CIO and its importance for the country's economy. For example, to assess the i-th vulnerability, the following indicator priority will be used: L4, L3, L2, L1, L5. The priority of indicators will be used to identify the most threatening CIO vulnerabilities.

Let us consider an example of a CIO in which 10 vulnerabilities were identified after analysis. After evaluation by CIO specialists and military experts, a set of indicator value tuples was created for all 10 vulnerabilities in the form of options:

1. ORGOG
2. GOORR
3. OGORG
4. ROGOO
5. OGGRO (2)
6. ROORG
7. ORGRO
8. RORORR
9. GOGGO
10. GRROR.

To identify the most threatening vulnerabilities, we will use lexicographic ordering of options (corridors of indicator ratings). After lexicographic ordering, we have:

9. GOGGO
2. GOORR
10. GRROR
5. OGGRO (3)
3. OGORG
1. ORGOG
7. ORGRO
4. ROGOO
6. ROORG
8. RORORR.

The most threatening vulnerabilities are located at the end of the sorted list of vulnerabilities. The most threatening is vulnerability 8, which has the following indicator values (L4, L3, L2, L1, L5): RORORR. However, due to limitations on the creation of defenses, in order to protect all 10 vulnerabilities, we will continue to form defensive actions for the vulnerabilities located at the end of the sorted list. To do this, with the help of experts, it is necessary to form a tuple of acceptable indicator values. For example, the tuple looks like this: OOOO.

Let's sort this tuple into a list. We get:

9. GOGGO
2. GOORR
10. GRROR
5. OGGRO (4)
3. OGORG

O O O O

1. ORGOG
7. ORGRO
4. ROGOO
6. ROORG
8. RORORR.

It follows that vulnerabilities 1, 7, 4, 6, and 8 can be classified as threatening and must be defended first.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Thus, this section analyzes the factors that influence the formation of vulnerabilities. Indicators have been developed to assess the impact of vulnerabilities on the state of critical infrastructure. Enemy attacks using strike drones lead to the excitation of vulnerabilities and the appearance of damage to critical infrastructure objects (partial or complete damage). To analyze and identify threatening vulnerabilities, qualitative assessments of indicators in the form of linguistic variable values were used. Threatening vulnerabilities were identified by lexicographic ordering of variants. The number of threatening vulnerabilities to be protected depends on the availability of defense resources, which is limited.

4. Building defense capabilities in the form of anti-drone means

Analysis of intelligence data and the opinions of military experts allow us to identify a number of critical infrastructure objects that could be the primary targets for massive wave attacks by enemy strike drones. To create a CIO defense that takes into account threatening vulnerabilities, it is necessary to assess the enemy's strike potential (F_j'') that will be used to attack the CIO. This is very important because when creating the appropriate defense potential (F_j'), it is necessary that ($F_j' \geq F_j''$). However, limited capabilities to allocate the necessary amount of anti-drone assets (air defense, electronic warfare, etc.) do not allow for full compliance with the requirement ($F_j' \geq F_j''$) for each j-th CIO, taking into account threatening vulnerabilities. Therefore, there is a difficult task of rationally allocating existing resources (air defense, electronic warfare, etc.), taking into account threatening vulnerabilities, to create the necessary defense. Let us form indicators that will be used to assess CIOs in conditions of martial law and limited capabilities to create a defense potential against wave attacks by enemy strike drones:

1. Defense potential for protecting the j-th CIO – F_j'.

2. Importance of the j-th CIO for the country's economy – α_j.

3. Risk of possible damage to the j-th CIO, taking into account threatening vulnerabilities – R_j.

For the rational allocation of anti-drone means (ADM) available for CIO defense, taking into account threatening vulnerabilities, we will use the integer (Boolean) programming method. Let us introduce the Boolean variable x_{jie}:

$$x_{jie} = \begin{cases} 1, \text{ if } e-\text{th ADM is allocated} \\ \quad \text{for defending } i-\text{th vulnerability} \\ \quad \text{of } i-\text{th CIO}, \\ 0, \text{ otherwise.} \end{cases} \qquad (5)$$

When allocating ADM resources, it is necessary to take into account existing restrictions on the creation of defense potential (F_j^*) for the j-th CIO, which is related to the impossibility of allocating them at present. Therefore, it is necessary to fulfill the requirement ($F_j' \leq F_j^*$), which affects the risk of damage to the j-th CIO (R_j), as a violation of the requirement ($F_j' \geq F_j''$) may occur.

Let us present the indicators of defense potential and the risk of possible damage to the CIO, taking into account the Boolean variable x_{jie}:

$$F' = \sum F_j' = \sum_{j=1}^{M} \sum_{i=1}^{m_j} \sum_{e=1}^{n_i} f_{jie} x_{jie}, \qquad (6)$$

where f_{jie} – defensive potential created with the help of e-th configuration of the ADM and allocated for protecting the location of the i-th vulnerability of the j-th CIO;

M – the number of CIOs that need to be protected from massive enemy attacks;

m_j – number of critical vulnerabilities in j-th CIO;

n_i – number of possible ADM facilities that can be allocated to protect the i-th vulnerability.

$$R = \sum_{j=1}^{M} R_j = \sum_{j=1}^{M} \sum_{i=1}^{m_j} \sum_{e=1}^{n_i} r_{jie} x_{jie}, \qquad (7)$$

where r_{jie} – risk of damage to the j-th CIO when the i-th vulnerability is exploited in an enemy drone attack, taking into account the e-th configuration of the ADM.

The following optimization problems can be formulated for the rational distribution of ADM for protecting a set of CIOs, taking into account their critical vulnerabilities:

1. Minimize the risk of damage to critical infrastructure, taking into account critical vulnerabilities:

$$\min R, \; R = \sum_{j=1}^{M} \sum_{i=1}^{m_j} \sum_{e=1}^{n_i} r_{jie} x_{jie}, \qquad (8)$$

with restrictions:

$$F_j' \leq F_j^*, \; F_j' = \sum_{i=1}^{m_j} \sum_{e=1}^{n_i} f_{jie} x_{jie}, \; j = \overline{1, M}. \qquad (9)$$

2. Maximize defense capabilities to protect critical infrastructure, taking into account the importance of individual facilities:

$$\max F', \; F' = \alpha_1 \sum_{i=1}^{m_1} \sum_{e=1}^{n_i} f_{1ie} + \alpha_2 \sum_{i=1}^{m_2} \sum_{e=1}^{n_i} f_{2ie} + \ldots + \ldots + \alpha_M \sum_{i=1}^{m_M} \sum_{e=1}^{n_i} f_{Mie}, \qquad (10)$$

with restrictions:

$$F_j' \le F_j^*,\ F_j' = \sum_{i=1}^{m_j}\sum_{e=1}^{n_i} f_{jie} x_{jie},\ j = \overline{1,M} \qquad (11)$$

$$R_j \le R_j^*,\ R_j = \sum_{i=1}^{m_j}\sum_{e=1}^{n_i} r_{jie} x_{jie},\ j = \overline{1,M}, \qquad (12)$$

where R_j^* – acceptable risk of damage to the j-th CIO, taking into account its importance.

Thus, this section sets out and resolves the task of forming the defense of critical infrastructure facilities against massive attacks by enemy strike drones, taking into account the existence of threatening vulnerabilities. Limited capabilities for allocating anti-drone assets have led to the need for their rational distribution among individual facilities, taking into account their importance. The indicators used to assess the distribution of anti-drone assets are in the form of defense potential and risks of facility damage. Limited capabilities to create the necessary number of anti-drone assets for defense affect the significance of the risks of damage. An optimization model was created for the rational distribution of anti-drone assets among critical infrastructure facilities using the integer Boolean programming method.

5. Multi-agent model for analyzing possible damage to critical infrastructure objects from enemy strike drone attack missions

The timing of an enemy attack mission using strike drones is an important factor influencing the planning of defensive measures to protect critical infrastructure, taking into account threatening vulnerabilities. The damage caused by an enemy attack depends on the number of threatening vulnerabilities that have been triggered and the fulfillment of protection conditions ($F_j' \ge F_j''$). Dynamic analysis of a possible enemy drone attack allows assessing the scale of CIO damage and the necessary preventive measures to minimize the risk of damage (R_j). Therefore, a simulation model was created, with the help of which, by simulating a possible enemy attack (flight of a swarm of strike drones), it is possible to plan preventive measures to protect the CIO, given the presence of threatening vulnerabilities. The simulation model was developed on the Any Logic platform and has an agent-based representation. The agents include:

1. Agent "map". Allows you to create a map to visualize the flight of a swarm of drones, marking their launch sites and the locations of vulnerable objects in the CIO.

2. "Drone swarm" agent. The characteristics of the strike drone swarm are formed (combat potential Fj", launch time, speed, possible movement distance, etc.).

3. "Vulnerabilities" agent. The characteristics of threatening vulnerabilities are formed (locations, possible anti-drone measures, etc.).

4. Defense agent. ADM resources are distributed according to CIO vulnerabilities with the formation of defense potential (F_j').

5. Swarm flight agent. The flight of a swarm of drones along a given route to the locations of vulnerabilities is simulated in time.

6. Agent "risk of damage". The risk value Rj is set for CIO vulnerabilities in terms of possible damage.

7. Agent "losses". Losses are formed when CIO damage occurs.

8. Agent "simulation control". Possible scenarios for a massive enemy drone attack are formed.

9. Agent "results." After simulation modeling, the following results are generated:

- time of the enemy's attack mission using a swarm of strike drones;
- enemy strike potential (F_j:");
- defensive potential for protecting CIO vulnerabilities (F_j');
- CIO damage risk (R_j);
- launch sites of enemy strike drones;
- locations of CIO vulnerabilities;
- damaged CIOs;
- scale of damage after CIO damage.

To ensure the reliability of the results, the simulation is performed multiple times. The results are averaged.

Fig. 1 shows a block diagram of the multi-agent model.

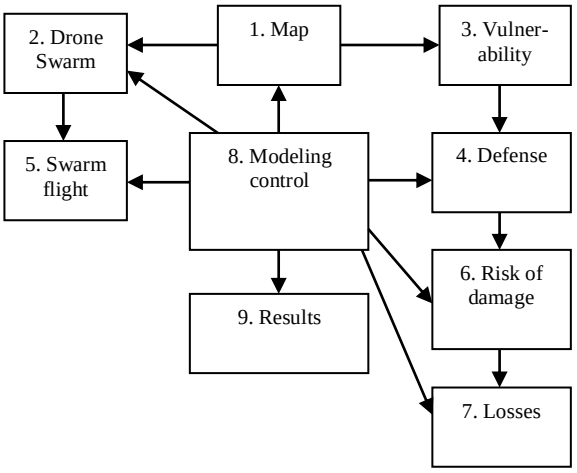

Fig. 1. Structural scheme of the multi-agent model

6. Discussion

A systematic representation of preventive measures for the protection of critical infrastructure (CIO) has been developed. Possible vulnerabilities arising during the operation of CIO have been analyzed.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Threatening vulnerabilities that affect the possible damage to CIO from enemy strike drone swarm attack missions have been identified. An assessment of the strike potential of enemy drone swarms (F_j") that the enemy will use when planning an attack, based on the locations of critical vulnerabilities of CIOs, has been carried out. An assessment of the creation of defensive potential (F_j') for the protection of CIOs, taking into account critical vulnerabilities, has been carried out. To create CIO defense using anti-drone measures (ADM), the requirement ($F_j' \geq F_j$") must be met. However, limited capabilities to allocate the necessary amount of ADM do not allow these requirements to be fully met for the entire set of CIOs. Therefore, a task arose, which was solved in the work on the rational distribution of ADM among the most important CIOs, taking into account threatening vulnerabilities. Multi-agent modeling was carried out, in time, of an enemy attack mission using a swarm of strike drones to analyze possible CIO damage after the attack. The modeling helps to assess the scale of damage and develop various scenarios for the enemy's attack mission.

The following research methodology is proposed:

- a systematic representation of the sequence of preventive measures for CIO defense;
- identification of threatening CIO vulnerabilities that can be exploited during a massive enemy attack using a swarm of strike drones;
- formation of the necessary defense potential (F_j') to ensure CIO protection, taking into account a possible enemy attack with the strike potential of drones (F_j");
- rational distribution of ADM resources according to the location of CIO vulnerabilities;
- minimization of the risk of damage (Rj) to particularly important CIOs;
- investigation of possible massive enemy attacks using strike drones with the help of multi-agent simulation modeling;
- formation of research results for analyzing the impact of threatening vulnerabilities and the scale of damage to CIOs from enemy drone attacks.

The relevance of the proposed approach is related to the need for scientific justification of the impact of threatening vulnerabilities on the possible damage to critical infrastructure objects due to enemy drone attacks.

The developed set of models is aimed at planning preventive measures to protect critical infrastructure facilities that have threatening vulnerabilities. This allows us to conclude that the proposed approach is timely and effective for creating protection for critical infrastructure facilities that have threatening vulnerabilities.

Future research will focus on improving applied information technology for modeling preventive measures to protect critical infrastructure from massive attacks by enemy strike drones. This will ensure active counteraction against an enemy focused on completely destroying the country's critical infrastructure.

7. Conclusions

The conducted research allows, through modeling, to analyze and plan preventive measures to protect critical infrastructure from massive wave attacks by enemy strike drones, namely:

- to form a logistical sequence of preventive measures for establishing security at critical infrastructure facilities;
- identify multiple threatening vulnerabilities in critical infrastructure facilities that could be exploited by enemy attacks;
- assess the strike potential and capabilities of the enemy to damage critical infrastructure with attack missions using strike drones;
- develop the necessary defense capabilities to protect critical infrastructure facilities, taking into account threatening vulnerabilities;
- carry out a rational distribution of anti-drone measures to reduce the risk of damage to critical infrastructure facilities;
- analyze various scenarios of enemy strike drone attacks to create the necessary defense of critical infrastructure facilities.

The scientific novelty of the proposed approach lies in the justification of protective measures for critical infrastructure against massive wave attacks by enemy strike drones based on the use of a developed set of original and new mathematical and simulation models.

Thus, the main conclusion of the study can be drawn:

The proposed set of models allows justifying the logical sequence of preventive measures to defend critical infrastructure facilities against massive attacks by enemy strike drones. This will ensure the effective use of available means of defense against enemy attacks under conditions of limited capabilities.

Contribution of authors: system analysis of the sequence of actions for creating defenses – **Oleg Fedorovich**; assessment of the enemy's capabilities to create strike potential – **Oleg Zamirets;** formation of the necessary defense potential for protection – **Oleksii Hubka**; optimization of defense means – **Yuliia Malieieva;** simulation modeling – **Andrii Popov;** experiments with model – **Andrii Rybka.**

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial,

personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This research was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All authors have read and approved the published version of this manuscript.

References

1. Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones*, 2022, vol. 6, is. 3, article no. 65. DOI: 10.3390/drones6030065.

2. .Chauhan, D., Kagathara, H., Mewada, H. Patel, S., Kavaiya, S., & Barb, G. Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies. *IEEE Access*, 2025, vol. 13, pp. 53476-53505. DOI: 10.1109/ACCESS.2025.3550338.

3. Osinga, F. P. B., & Roorda, M. P. From Douhet to Drones, Air Warfare, and the Evolution of Targeting. In: Ducheine, P., Schmitt, M., Osinga, F. (eds) *Targeting: The Challenges of Modern Warfare*. T.M.C. Asser Press, The Hague, 2016, pp. 27-76. DOI: 10.1007/978-94-6265-072-5_3.

4. Luo, X., Wu, Y., & Wang, F. Target Detection Method of UAV Aerial Imagery Based on Improved YOLOv5. *Remote Sensing*, 2022, no. 14(19), article no. 5063. DOI: 10.3390/rs14195063.

5. Fedorovych, O., Kritskiy, D., Malieiev, L., Rybka, K., & Rybka, A. Military logistics planning models for enemy targets attack by a swarm of combat drones. *Radioelectronic and Computer Systems*, 2024, no. 1, pp. 207-216. DOI: 10.32620/reks.2024.1.16.

6. Zmysłowski, D., Skokowski, P., & Kelner, J. M. Anti-drone sensors, effectors, and systems – a concise overview. *TransNav: International Journal on Marine Navigation and Safety of Sea* Transportation, 2023, no. 17(2), pp 455-461. DOI: 10.12716/1001.17.02.23.

7. Tytarenko, O., & Vlasenko, Ye. Protypovitriana oborona v rosiisko-ukrainskii viini: uroky ta rekomendatsii [Air defence in the russian-ukrainian war: lessons and recommendations]. *Povitriana mits Ukrainy – Air power of Ukraine*, 2024, no. 1(6), pp. 49–55. DOI: 10.33099/2786-7714-2024-1-6-49-55. (in Ukrainian).

8. Shin, M. J., Yoon, S. S., & Euom, I. C. A Study on the Method of Vulnerability Analysis of Critical Infrastructure Facilities. *Journal of the Korea Institute of Information Security & Cryptology*, 2022, no. 32(2), pp. 243-253. DOI: 10.13089/JKIISC.2022.32.2.243.

9. Pytel, M., & Cieśla, M. Use of Territorial Defense Forces (TDF) in combat operations. *Scientific Journal of the Military University of Land Forces*, 2021, no. 53(1 (199), pp. 61-72. DOI: 10.5604/01.3001.0014.8110.

10. Semenenko, O., Deineha, O., Voronchenko, I., Borysiuk, S., Mytchenko, S., & Taran, O. On the Question of Transformation of Forms and Methods of Military Actions in the Conditions of Hybrid Wars. *Social Development and Security*, 2021, vol. 11, no. 2, pp. 256-271, DOI:10.33445/sds.2021.11.2.22.

11. Kang, H., Joung, J., Kim, J., Kang J., & Cho, Y.S. Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems. *IEEE Access*, 2020, vol. 8, pp. 168671-168710. DOI: 10.1109/ACCESS.2020. 3023473.

12. Tyurin, V,. Martyniuk, O., Mirnenko, V., Open'ko P., & Korenivska, I. General Approach to Counter Unmanned Aerial Vehicles. *IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, Kiev, Ukraine, 2019, pp. 75-78, DOI: 10.1109/ APUAVD47061.2019.8943859.

13. Fedorovich, O., Lukhanin, M., Prokhorov, O., Slomchynskyi, O., Hubka, O., & Leshchenko, Yu. Simulation of arms distribution strategies by combat zones to create military parity of forces. *Radioelectronic and computer systems*, 2023, no. 4, pp. 209-220. DOI: 10.32620/reks.2023.4.1.

14. Lyu, C., & Zhan, R. Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle. *IEEE Aerospace and Electronic Systems Magazine*, 2022, vol. 37, no. 1, pp. 6-31. DOI: 10.1109/MAES.2021.3115205.

15. Park, S., Kim, H. T., Lee, S., Joo H., & Kim, H. Survey on Anti-Drone Systems: Components, Designs, and Challenges, *IEEE Access*, 2021, vol. 9, pp. 42635-42659. DOI: 10.1109/ACCESS.2021. 3065926.

16. Kim, J., Choi, J., & Kwon, H. A study on the development directions of a smart counter-drone defense system based on the future technological environment. KSII *Transactions on Internet and Information Systems* (TIIS), 2024, no. 18(7), pp. 1929-1952. DOI: 10.3837/tiis.2024.07.011.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

17. Di Pietro, R., Raponi, S., Caprolu, M., & Cresci, S. Critical Infrastructure. In: *New Dimensions of Information Warfare.* Advances in Information Security, 2021, vol 84, pp. 157-196. Springer, Cham. DOI: 10.1007/978-3-030-60618-3_5.

18. Dreis, Yu., & Derkach, O. L. Bazova mnozhyna uzahalnenykh kryteriiiv vidnesennia ob'iektiv do krytychnoi infrastruktury derzhavy [Basic set of generalized criteria for assigning objects to the critical infrastructure of state]. *Bezpeka informatsii – Ukrainian Scientific Journal of Information Security*, 2021, vol. 27, no. 1, pp. 13–20. Available at: http://repository.mu.edu.ua/jspui/handle/123456789/5217. (accessed 12.3.2025). (in Ukrainian).

19. Enrico, Zio. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 2016, vol. 152, pp. 137-150. DOI: 10.1016/j.ress.2016.02.009.

20. Ewa, W. O., Ugwu, O. O. & Okafor, F. O. Resilient–vulnerability analysis of critical infrastructure, key resources, assets, and facilities. *Innovative Infrastructure Solutions*, 2024, no. 9, article no. 109 DOI: 10.1007/s41062-024-01405-9.

21. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., & Chopenko, D. A development of a concept for building critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, 2021, vol. 3, no. 111(9), pp. 63–83. DOI: 10.15587/1729-4061.2021.233533.

22. Llinas, J. & Sentz, K. Knowing the Enemy, Dealing with Deception, and Situation/Threat Estimation. 2024 *IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Montreal, QC, Canada, 2024, pp. 31-38. DOI: 10.1109/CogSIMA61085.2024.10554049.

23. Shalyhin, A. A., Nerubatskyi, V. O., & Smyk, S. I. Metodychnyi pidkhid do otsinky boiovykh potentsialiv bezpilotnykh aviatsiinykh kompleksiv, yikh pidrozdiliv i uhrupovan [Methods of assessment of combat potentials of unmanned aircraft systems, their divisions and groups]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy – Science and technology of the Air Forse of Ukraine*, 2021, no. 2 (43), pp. 73-79. DOI: 10.30748/nitps.2021.43.10. (in Ukrainian).

24. Shovkoshytnyi, I., & Vasylenko, O. Vybir pokaznykiv otsiniuvannia efektyvnosti zastosuvannia roiv udarnykh bezpilotnykh litalnykh aparativ dlya urazhennia nestatsionarnykh hrupovykh tsilei [Selection of indicators for assessing the effectiveness of the use of swarms of striking unmanned aerial vehicles to defeat non-stationary group targets]. *Povitriana mits Ukrainy – Air power of Ukraine*, 2024, no. 2(7), pp. 61–72. DOI: 10.33099/2786-7714-2024-2-7-61-72. (in Ukrainian).

25. Horbenko, V., & Kireienko, V. Metodyka vyznachennia vazhlyvosti ob'iektiv protypovitrianoi oborony v protsesi planuvannia operatsiy z vykorystanniam metodu faktornoho analizu [Method of determining the importance of air defense objects in the operations planning process using the method of factor analysis]. *Povitriana mits Ukrainy – Air power of Ukraine*, 2024, no. 2(7), pp. 36–42. DOI: 10.33099/2786-7714-2024-2-7-36-42. (in Ukrainian).

26. Lenkov, S., Kryvtsun, V., Miroshnichenko, O., Holushko, S., & Koltsov, R. Analiz stanu rozvytku pytannia zakhystu ob'iektiv krytychnoi infrastruktury z vykorystanniam inzhenernykh boieprypasiv [Analysis of the state of development of the issue of protection of critical infrastructure facilities using engineered munitions]. *Pidvodni Tekhnolohii – Underwater technologies: Industrial and Civil Engineering*, 2023, no. 13, pp. 81–91. DOI: 10.32347/uwt.2023.13.1803. (in Ukrainian).

27. Koval, M. V., Koval, V. V., Kotsuruba, V. I., & Bilyk, A. S. Orhanizatsiino-tekhnichni zasady pobudovy systemy inzhenernoho zakhystu ob'iektiv krytychnoi infrastruktury enerhetychnoi haluzi Ukrainy [Organizational and technical principles of construction of a system of engineering protection of critical infrastructure objects of the energy industry of Ukraine]. *Nauka i oborona – Science and Defence*, 2022, no. 3-4, pp. 11-16. DOI: 10.33099/2618-1614-2022-20-3-4-11-16. (in Ukrainian).

28. Pavlov, D., Sukonko, S., & Salna, N. Mozhlyvosti ta problemni pytannia udoskonalennia zakhystu ob'iektiv infrastruktury u suchasnykh umovakh. [Opportunities and problems in improving the protection of critical infrastructure objects in modern conditions]. *Chest i zakon – Honor and Law*, 2022, no. 4(83), pp. 67-74. DOI: 10.33405/2078-7480/2022/4/83/272291. (in Ukrainian).

29. Pascarella, D., Gigante, G., Vozella, A., Bieber, P., Dubot, T., Martinavarro, E., Barraco, G., & Li Calzi, G. A Methodological Framework for the Risk Assessment of Drone Intrusions in Airports. *Aerospace*, 2022, no. 9(12), article no. 747. DOI: 10.3390/aerospace9120747.

30. Savchenko, I. O., & Matsko, P. I. Systemnyi pidkhid do pidtrymky pryiniattia rishen shchodo zahroz krytychnii infrastrukturi z vykorystanniam metodiv ekspertnoho otsiniuvannia [A systematic approach to supporting decision-making on threats to the critical infrastructure using expert assessment methods]. *Vcheni zapysky, Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho* – Scientific Notes of V.I. Vernadsky Taurida National University, 2025, vol. 36 (75), no. 2, part 2, pp. 199-205. DOI: 10.32782/2663-5941/2025.2.2/27. (in Ukrainian).

Надійшла до редакції 10.06.2025, розглянута на редколегії 18.08.2025

МОДЕЛЮВАННЯ ЗАГРОЗЛИВИХ ВРАЗЛИВОСТЕЙ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЛЯ СТВОРЕННЯ ОБОРОНИ ВІД ХВИЛЬОВИХ АТАК РОЮ УДАРНИХ ДРОНІВ

О. Є. Федорович, О. М. Замірець, А. В. Попов, О. С. Губка, Ю. А. Малєєва, А. В. Рибка

Сучасні технології, які використовуються у гібридній війні, дозволяють проводити противнику масштабні атакуючі дії за об'єктами критичної інфраструктури (транспорт, енергетика, промислові підприємства, тощо), що впливає на погіршення стану економіки країни. Використання противником БПЛА, у вигляді хвиль рою ударних дронів, різко підвищило ризики ураження об'єктів критичної інфраструктури (ОКІ), які деградують у часі та мають загрозливі вразливості. Тому, **актуально** проведення дослідження щодо моделювання оборонних заходів для охорони ОКІ від масованих повітряних атак противника. **Предметом** дослідження, в публікації, є математичні та імітаційна моделі, які створюються для планування превентивних заходів щодо оборони ОКІ. **Метою** дослідження є створення комплексу моделей, за допомогою яких можна аналізувати та виявляти загрозливі вразливості об'єктів критичної інфраструктури, які збуджуються при хвильових атаках ударних дронів противника, планувати відповідні оборонні дії превентивного характеру, в умовах обмежених можливостей. **Завдання,** які необхідно вирішити: провести системний аналіз послідовності дій щодо планування оборони ОКІ; виявити найбільш загрозливі вразливості ОКІ, місця яких можуть бути атаковані противником; зробити раціональний розподіл оборонного потенціалу для захисту ОКІ, з урахуванням можливостей противника щодо створення ударного потенціалу, з використанням бойових дронів; розробити мультиагенту імітаційну модель для аналізу можливих уражень ОКІ місць масованих атак ударних дронів. Використані математичні **методи та моделі:** системний аналіз превентивних заходів для створення оборони ОКІ; якісне оцінювання показників ОКІ для пошуку загрозливих вразливостей; лексикографічне впорядковування варіантів для виявлення множини актуальних ОКІ, які підлягають обороні; цілочисельна (булева) оптимізація для раціонального розподілу обмеженого оборонного потенціалу за місцями розташування загрозливих вразливостей ОКІ; мультиагентне імітаційне моделювання хвильових дронових атак противника для аналізу уражень ОКІ. Отримані **результати:** сформована логістична послідовність превентивних заходів щодо оборони ОКІ; виявлена множина загрозливих вразливостей в ОКІ; проаналізовано ударний потенціал та можливості противника щодо ураженості ОКІ; сформований потрібний оборонний потенціал для захисту ОКІ; проведено раціональний розподіл протидронових засобів для зменшення ризиків ураження ОКІ; промодельовані різні сценарії атак ударних дронів та можливі ураження ОКІ. **Висновки:** запропонований комплекс моделей дозволяє обґрунтувати логістичну послідовність проведення превентивних заходів щодо створення оборони ОКІ від масованих хвильових атак ударних дронів противника. Це забезпечить ефективність використання наявних протидронових засобів оборони від атакуючих дій противника, в умовах обмежених можливостей. **Наукова новизна** запропонованого підходу полягає в обґрунтуванні захисних дій щодо об'єктів критичної інфраструктури від масованих хвильових атак ударних дронів противника на основі використання розробленого комплексу оригінальних та нових математичних та імітаційної моделей.

Ключові слова: вразливості критичної інфраструктури; превентивні заходи щодо створення оборони; хвильові атаки ударних дронів; якісне оцінювання вразливостей; лексикографічне впорядковування варіантів; оптимізація розподілу оборонного потенціалу; мультиагентне моделювання хвильових дронових атак.

Федорович Олег Євгенович – д-р техн. наук, проф., зав. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Замірець Олег Миколайович – канд. техн. наук, головний конструктор Державного підприємства Науково-дослідний технологічний інститут приладобудування, Харків. Україна.

Попов Андрій Вячеславович – канд. техн. наук, доц., доц. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Губка Олексій Сергійович – канд. техн. наук, доц., доц. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Малєєва Юлія Анатоліївна – канд. техн. наук, доц., доц. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Рибка Андрій Вікторович – асп. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Oleg Fedorovich – Doctor of Technical Sciences, Professor, Head of the Department of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: o.fedorovych@khai.edu, ORCID: 0000-0001-7883-1144.

Oleg Zamirets – PhD, Chief Technology Officer, State Enterprise Scientific Research Technological Institute of Instrument Engineering (SE SRTIIE), Kharkiv, Ukraine,
e-mail: nitip@ukr.net, ORCID: 0000-0001-5902-2501.

Andrei Popov – Candidate of Technical Science, Associate Professor, Associate Professor at the Department of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: a.popov@khai.edu; ORCID: 0000-0001-8984-731X.

Oleksii Hubka – Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: o.gubka@khai.edu, ORCID: 0009-0009-7954-5639.

Yuliia Malieieva – Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: juliabelokon84@gmail.com, ORCID:0000-0003-3553-9156.

Andrii Rybka – PhD Student of the Department of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: kafius@ukr.net.