UDC 005.963.1:629.7.-027.3 **doi: 10.32620/reks.2025.3.01**

Oleg FEDOROVICH[1], Olga MALYEYEVA[1], Andrii HUMENNYI[1], Oleksandr LESHCHENKO[1], Yuliia LESHCHENKO[1], Ganna PLIEKHOVA[2]

[1] ***National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine***
[2] ***Kharkiv National Automobile and Highway University, Kharkiv, Ukraine***

MODELING OF DEFENSIVE ACTIONS FOR PROTECTING MILITARY AND CIVILIAN FACILITIES FROM MASSIVE WAVE ATTACKS BY ENEMY STRIKE DRONES

The conditions of modern hybrid warfare require the creation of the necessary defense potential to protect military facilities and critical infrastructure from massive attacks by enemy strike drones. A feature of repelling drone air attacks is the use of a diverse arsenal of defensive means (anti-drone means (ADM), electronic warfare (EW), anti-aircraft warfare (AAW), interceptor drones (ID), etc.). Therefore, it is ***relevant*** *to conduct research on modeling defensive actions and planning the protection of military and civilian facilities from attacking missions of enemy strike drones. The* ***subject*** *of the study is a mathematical and simulation model used for planning the protection of military and civilian facilities against swarm attacks by enemy strike drones.The* ***purpose*** *of the study is to simulate the planning of defensive actions against enemy air attacks, under conditions of limited capabilities, which will ensure the rational use of military resources.* ***Tasks*** *to be solved: analyze the sequence of defensive actions; analyze the most threatening places for the formation and launch of enemy strike drones; justify the creation of the defense of critical military and civilian facilities; create the necessary defense potential to protect critical military and civilian facilities; model possible scenarios for the launch and movement of enemy strike drones; demonstrate the feasibility and effectiveness of the proposed approach using an illustrated example. Mathematical* ***methods and models*** *used: system analysis of defensive anti-drone actions; qualitative assessment of defensive action options using linguistic variables; lexicographic ordering of options to highlight relevant locations for the protection of military and civilian facilities; integer (boolean) programming method to substantiate the defensive potential of protection, in conditions of limited capabilities; multi-agent modeling to analyze and predict possible scenarios of an enemy attack mission using strike drones. The following* ***results*** *were obtained: a systematic presentation of planning defensive actions against massive attacks by enemy strike drones was proposed; the most threatening places for the formation and launch of swarms of enemy strike drones were substantiated; the relevant locations of anti-drone means for protecting military facilities and dual infrastructure facilities were identified; the necessary defense potential was created to protect against air attacks in conditions of limited capabilities; a multi-agent simulation model was developed to analyze and predict possible scenarios for the launch and flight of enemy strike drones to the locations of critical military and civilian facilities.* ***Conclusions.*** *The results of the study allow us to substantiate and plan defensive anti-drone actions to protect military facilities and dual-purpose infrastructure facilities. The* ***scientific novelty*** *of the proposed approach lies in the scientific substantiation of defensive actions to protect military and civilian facilities from massive attacks by enemy strike drones based on the use of the developed complex of original and new mathematical and simulation models.*

Keywords: *anti-drone defense; justification of threatening launch sites of enemy strike drones; protection of military and civilian facilities; optimization of the defense potential of protection against strike drones; linguistic variables for qualitative expert assessments; lexicographic ordering of options; multi-agent simulation modeling of strike drone attacks.*

1. Introduction

A new innovative tool of war, in the form of unmanned aerial vehicles (UAVs), is widely used by the enemy to carry out attack missions [1]. Therefore, it is necessary to create an active air shield to protect against massive attacks by enemy strike drones. The appearance of drones of various purposes in combat operations requires the creation of a system for countering enemy attacks on the ground and in the air [2]. The success of operational and tactical actions depends on creating proper conditions for the military on the battlefield [3, 4]. Currently, it is possible to create an active shield to counter the enemy using anti-drone means (ADM), (in the form of electromagnetic, pulsed devices, laser weapons, etc.), electronic warfare (EW), anti-aircraft defense (anti-aircraft weapons, large-caliber machine guns, tactical missiles, etc.), interceptor drones (ID)

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

[5, 6]. Their use requires planning defensive actions to counter enemy attack missions. Therefore, a difficult task arises in terms of planning defensive actions using means (ADM, EW, AAW, ID) that can create an active air defense shield for conducting successful combat operations on the battlefield. It is necessary to form the necessary combat potential for defense against massive enemy attacks, when planning defensive anti-drone actions [7, 8]. The use of regular monitoring of military situations on the battlefield, with the help of reconnaissance drones, makes it possible to detect the places of formation and launch of swarms of enemy attack drones, accumulations of military equipment, control points of attack drone flights, etc. Thus, intelligence provides an opportunity to assess the enemy's combat potential and form the appropriate defensive potential of means (ADM, EW, AAW, ID) to conduct active countermeasures against enemy air attacks [9, 10]. When forming a set (ADM, EW, AAW, ID), it is necessary to predict the enemy's activity and its possible preparation for attacking actions with strike drones. Means (ADM, EW, AAW, ID) must be concentrated in places that will allow for the defense of critical military and civilian facilities [11, 12]. Also, it is necessary to take into account the limited possibilities of use (ADM, EW, AAW, ID) to form their plurality to ensure the necessary defensive potential to counter the enemy in the air.

Taking into account the above, we can conclude that it is relevant to conduct a study on planning defensive anti-drone actions using means (ADM, EW, AAW, ID) to protect military facilities and dual-purpose infrastructure.

1.1. Motivation

Planning defensive actions against massive enemy attacks using strike drones is a difficult task, as it is necessary to take into account the dynamics of changes in military circumstances on the battlefield, the presence of the enemy's combat strike potential in the form of a multitude of drones, and the creation of the necessary defensive anti-drone potential of means (ADM, EW, AAW, ID) [13, 14]. When creating a set of means (ADM, EW, AAW, ID), it is necessary to take into account their diversity and quantity, depending on the possible directions of massive enemy drone attacks [15, 16].

Therefore, it is urgent to solve the problem of planning the necessary means (ADM, EW, AAW, ID) to create an active shield to counter enemy air attacks.

1.2. State of the art and problem statement

There are a number of problems that have arisen and are related to the rational use of means (ADM, EW, AAW, ID) to create anti-drone defense. Part of the problem is solved, but there are new problems that need to be investigated. Consider an analysis of studies related to the following issues:

1. Real-time monitoring of changes in the military situation on the battlefield.

The article [17] considers the issues of supporting the decision-making process using the Internet of Things network, based on information collected from the battlefield and transmitted to command, control, communications, computing, intelligence, and surveillance systems. A context-aware environmental monitoring system is presented that uses real-time battlefield information to increase the resilience and survivability of military networks.

The study [18] solves the problem of periodic monitoring of the battlefield. A “reasonable” monitoring interval is established, the discriminant of which is derived according to the commanders’ requirements for signal accuracy.

2. Formation of the necessary defense potential (ADM, EW, AAW, ID) to provide countermeasures against massive attacks by enemy strike drones.

This issue is solved by the authors of the paper [19] by forecasting the possible form of the "algorithmized" battlefield, taking into account the use of the land component on a technologically saturated battlefield in conditions of high-intensity conflict.

The article [20] developed a new concept of countermeasures systems capable of identifying and neutralizing several enemy drones classified as a threat. A multi-platform anti-UAV system based on a team of mini-drones acting as a cooperative defense system is proposed.

3. Location of means (ADM, EW, AAW, ID) for effective protection of military and civilian facilities from enemy drone attacks.

Incorporating individual aspects of EW into the operational capability assessment model is an important and complex task, which is discussed in the article [21]. An optimization model is presented for determining the structure of the EW support modules with the desired capabilities, which allows for the implementation of the defined operational concepts taking into account the operational and cost criteria. A method of modifying the assessment of the parties' potentials as a result of the impact of EW for the distribution of support units during the formation of own forces in response to the potential formation and actions of the enemy is presented. The authors of the paper [22] investigate the task of optimizing the deployment of air defense systems against reconnaissance drone swarms. Given a set of available AAW, the problem determines the location of each AAW in a predefined region in such a way that the

cost of enemy drones flying through that region is maximized.

4. Taking into account existing restrictions on the use of means (ADM, EW, AAW, ID) and the successful conduct of anti-drone operations [23, 24].

The authors of the paper [23] note that creating a military-grade anti-drone system for every private or public facility is unaffordable due to the costs of installation and operation.

Accordingly, the article [24] proposes the integration of EW means with reconnaissance and fire control means in a unified information and communication space, the creation of radio reconnaissance systems, improvement of the signal monitoring system. This makes it possible to better detect and block electronic threats, increase the effectiveness of anti-EW methods, and improve the methods of coding and encryption of information.

5. Difficulties in assessing the required number of means (ADM, EW, AAW, ID) for use in each separate location for protecting military and civilian facilities, depending on a possible enemy drone attack.

The article [25] proposes an approach to planning the operational capabilities of the support modules of the armed forces, including EW units.

The authors of the paper [26] proposed a method that classifies electronic warfare systems and defines elements for measuring the effectiveness of each system, taking into account the characteristics of cyberspace to assess the damage caused by cyberattacks.

6. Determination of critical and threatening places of formation and launch of enemy attack drones, in the conditions of conducting reconnaissance with possible countermeasures of the enemy.

In article [27] a methodological framework for assessing the risk of drone incursions into airports is proposed, adapted to the specifics of the attack, the characteristics of the airport and the current operation, as well as taking into account reasons related to both safety and security. An airport vulnerability index is calculated. A set of event trees is defined to assess the risks of different threat scenarios.

The authors of the paper [28] apply an agent approach to implementing joint threat intervention among several network agents in the form of a swarm of drones with combat and communication capabilities. This research combines AI-based decision-making methods for a swarm of companion drones capable of providing effective defensive actions in cooperative and autonomous modes.

More attention in articles [29, 30] is paid to the technological aspect of the production of weapons (drones) to create a defense potential.

This is an incomplete list of problems and ways to solve them, which continue to be replenished with new ones in the conditions of modern hybrid warfare, which indicates the relevance of conducting research on planning defensive actions to reflect attacks by enemy strike drones.

An analysis of publications on these issues has shown the complexity of the task of planning defensive actions to support the military on the battlefield [31, 32].

This article presents solutions to some of the specified topical problems.

1.3. Objectives and methodology

There is a contradiction between the need to create an active anti-drone shield against attacking missions by enemy strike drones and the imperfection of existing methods, models and information technologies that would allow, to the full extent, to conduct a systematic analysis of a set of defensive actions, using means (ADM, EW, AAW, ID) to reflect enemy attacks; to form rational locations (ADM, EW, AAW, ID) and their necessary number for the defense of military and civilian facilities; to form the necessary defense potential to reflect enemy air attacks.

The purpose of the research is to create a set of models that can be used to analyze and plan actions to create defenses for military and civilian facilities against massive enemy air attacks.

In accordance with the stated research goal, it is necessary to solve the following tasks:

1. To carry out a systematic analysis of defensive actions regarding the display of enemy attacks using strike drones.

2. Analyze possible locations and launch sites for enemy strike drones, identifying the most threatening ones.

3. To justify the creation of defense for critical military and civilian facilities from massive attacks by enemy strike drones.

4. Taking into account limited capabilities, to form the necessary defensive potential of means of combating drones.

5. Develop a multi-agent simulation model for the analysis of possible scenarios of massive attacks by enemy strike drones.

6. Provide an illustrated example of the rational distribution of defense means to protect critical facilities from enemy strike drone attacks.

The article is organized as follows:

Section 2 is devoted to a systematic analysis of actions to create defense and protect military and civilian facilities from attacks by enemy strike drones.

Section 3 is related to the justification of threatening locations and launches of enemy strike drones.

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

Section 4 is devoted to the justification of the current locations of anti-drone defense means for military and civilian facilities.

Section 5 is devoted to the rational distribution of defense potential, in the form of anti-drone means, to ensure effective defense.

Section 6 is devoted to the creation of a multi-agent model and the analysis of possible enemy attack scenarios and the planning of anti-drone actions.

Section 7 illustrates, by example, the feasibility and effectiveness of the proposed approach.

Section 8 contains a discussion of scientific results and their presentation in the form of a methodology, which allows emphasizing the significance of the research for practical application.

Section 9 concludes the article by summarizing the conclusions, providing a perspective for further research and the creation of applied information technology for planning defensive actions to counter enemy drone attacks.

2. Systematic analysis of defensive operations to reflect enemy attacks using strike drones

The enemy's preparation for offensive actions is associated with the formation of units that create and launch swarms of attack drones to carry out massive attacks on the locations of military facilities (MF) (command posts, communications centers, military equipment clusters) and civilian facilities (CF) (bridges, railway stations, warehouses, industrial enterprises, etc.).

For effective defense of locations (MF, CF), it is necessary to create a defensive potential of anti-drone means (ADM, EW, AAW, ID), taking into account the enemy's capabilities for attacking actions, using strike drones. Therefore, it is necessary to form a sequence of logistical actions to create defense of locations (MF, CF) from massive attacks by enemy strike drones. We will form a sequence of logistical actions to protect objects (MF, CF) from massive attacks by enemy strike drones in the form of:

1. Conducting reconnaissance activities to identify possible locations and launch sites of enemy strike drones (LLSESD). Reconnaissance can be both airborne (reconnaissance drones) and on the battlefield.

The regularity of monitoring conditions on the battlefield makes it possible to obtain up-to-date information on possible locations (LLSESD) in conditions of dynamic changes in military circumstances. The availability of such information, with an assessment of its reliability, allows you to create a map with the location of a set of enemy locations (LLSESD), which may be used to carry out attacks on objects (MF, CF).

2. Formation of possible directions of massive enemy drone attacks. This allows rational distribution of resources (ADM, EW, AAW, ID) to reflect enemy drone attacks.

3. Limited opportunities for creating a full-fledged defense of all locations (MF, CF) lead to the need to consider only those locations (LLSESD) of the enemy that pose the greatest threat to objects (MF, CF). Therefore, the task arises of substantiating the set of those places (LLSESD) that have the highest level of threats to objects (MF, CF).

4. It is necessary, with the help of intelligence and military experts, to assess the combat potential (P′′) of the enemy, taking into account the locations (LLSESD), which have a high level of threats, in order to substantiate defensive actions regarding the protection of critical objects (MF, CF).

5. Next, it is necessary to justify a set of critical objects (MF, CF) for which, first of all, it is necessary to create defense against massive attacks by enemy strike drones.

6. Next, form a set of defense means to reflect massive attacks by enemy strike drones. For this purpose, anti-drone means in the form of (ADM, EW, AAW, ID) can be used. The composition of means (ADM, EW, AAW, ID) is formed depending on the characteristics of the objects (MF, CF), as well as the limited conditions for removing the necessary number of means (ADM, EW, AAW, ID) for defense.

7. It is necessary to justify the defense potential (P′) in terms of means (software, electronic warfare, air defense, air defense). The effectiveness and success of defensive actions depends on the possibility of creating conditions ($P' \geq P''$). But, due to limited possibilities, for some objects (MF, CF), these conditions will not be fulfilled. This leads to the search for priority locations for objects (MF, CF), for which it is necessary, first of all, to plan defensive actions.

8. Creation of a flight map for modeling and predicting the movement of enemy strike drones and the locations of objects (MF, CF).

9. Formation and analysis of possible scenarios of enemy attack actions using a swarm of strike drones.

10. Modeling and predicting the results of an attack by enemy strike drones on objects (MF, CF).

11. Assessment of the effectiveness of the actions of means (ADM, EW, AAW, ID) in repelling the attack and destroying enemy strike drones.

The presented list of actions may be supplemented with new actions as technological innovations emerge in modern hybrid warfare, using swarms of strike drones.

Thus, it can be argued that there is a need to form a complex of analytical and simulation models that will

allow analyzing, modeling and predicting the success of defensive actions to protect military and civilian facilities from enemy air attacks using strike drones.

This section has created a sequence of logistical actions to establish active protection of military facilities and civilian critical infrastructure facilities from massive attacks by enemy strike drones. A conclusion was made regarding the need to create a complex of models for the analysis and planning of defensive actions against air attacks by enemy attack drones.

3. Analysis of possible locations and launches of enemy strike drones with the identification of the most threatening

To create an air shield of defense against attack drone attacks, it is necessary, with the help of reconnaissance drones, to determine possible locations and launch sites of enemy UAVs (LLSESD). For each i-th location (LLSESD), it is necessary to assess the level of threat to military and civilian facilities (MF, CF) using the following indicators:

- the distance of the enemy's i-th location (LLSESD) from the front line (L_i);

- flight time of a swarm of drones from the i-th location (LLSESD) of the enemy to the objects (MF, CF) (T_i);

- combat potential of a swarm of attack drones (depends on the type of drones and their number), which is formed in the i-th location (LLSESD) (W_i);

- assessment of the risk of an attack by enemy strike drones from the i-th location (LLSESD) (R_i).

It should be noted that a set of indicators may be distributed, depending on the conditions of hostilities and the creation of defensive measures.

For each i-th location (LLSESD) of the enemy, these indicators have their own values. It is also necessary to take into account the priority of indicators, depending on the characteristics of the objects (MF, CF) that can be attacked by enemy drones.

The number of enemy locations (LLSESD) identified by reconnaissance may be such that it is necessary to select the most threatening ones from their entire set, using the values of the indicators (L_i, T_i, W_i, R_i) and their priority. To identify threatening enemy locations (LLSESD) from the possible sets, we will use a simpler representation of the indicators in the form of qualitative assessments that military experts are able to form based on intelligence.

Let us introduce a linguistic variable y_{ik}, where the index «i» is used for the i-th location (LLSESD) of the opponent, and the index «k» for the value of the k-th indicator. Let's represent qualitative assessments in the form of letters of the Latin alphabet:

$$y_{ik} = \begin{cases} \text{G – the threat level is "green",} \\ \text{which means it exists, but is small;} \\ \text{O – the threat level is "orange",} \\ \text{which means a large threat;} \\ \text{R – the threat level is "red",} \\ \text{which means a very large threat.} \end{cases} \quad (1)$$

Thus, each possible location (LLSESD) of the enemy can be evaluated using the values of the indicators (L_i, T_i, W_i, R_i), taking into account their priority.

Let us consider an illustrated example of using qualitative assessments to analyze a set of enemy locations (LLSESD) that were detected by reconnaissance. Each i-th location (LLSESD) of the enemy will be represented as a tuple of assessments (L_i, T_i, W_i, R_i), taking into account the priority of indicators in each i-th (LLSESD). For example, let's take 10 enemy locations (LLSESD) that were evaluated by military experts:

1. G O R O	6. O R O R	
2. O G G R	7. R O G G	
3. G O O R	8. G O R G	(2)
4. R G O O	9. O G O G	
5. O R G G	10. R O G O.	

The presented set of enemy location options (MRZUD) is ordered according to the values of the indicators (Li, Ti, Wi, Ri) and the method of lexicographic ordering of options.Then we get the answer:

3. G O O R	5. O R G G	
8. G O R G	6. O R O R	(3)
1. G O R O	4. R G O O	
2. O G G R	7. R O G G	
9. O G O G	10. R O G O.	

Note that at the beginning of the ordered list are the enemy's location options (LLSESD) that have the lowest threat level, and at the end are the enemy's location options (LLSESD) with the highest threat level. It should be noted that option 10 has the greatest military threat with ratings (R O G O) for facilities (MF, CF). This affects the creation of a system for protecting facilities (MF, CF) in the form of a set of means (ADM, EW, AAW, ID), the number of which may be limited. Therefore, it is necessary to select the required number of enemy threat locations (LLSESD) to create a defense against them. It is simpler to choose a limit on the number of enemy threatening locations (LLSESD). For example, we will create a defense of objects (MF, CF) from 4 possible enemy threatening locations (LLSESD). Then we will get the following options:

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

6. O R O R
4. R G O O (4)
7. R O G G
10. R O G O.

However, it is possible to use a tuple of threshold values of the indicator estimates (L_i, T_i, W_i, R_i) in relation to the threat level in the form, for example, $\boxed{\text{O O O O}}$. We order the threshold tuple among the set of location options (LLSESD) of the enemy:

3. G O O R
8. G O R G
1. G O R O
2. O G G R
9. O G O G
$\boxed{\text{O O O O}}$ (5)
5. O R G G
6. O R O R
4. R G O O
7. R O G G
10. R O G O.

As a result, we will get a set of options (5, 6, 4, 7, 10) that must be used to create a system for protecting objects (MF, CF) from swarm attacks by strike drones.

Thus, in this section, the task was considered and a solution was formed to justify the threatening locations and launch of enemy strike drones, which contributes to the creation of the necessary defense of military and civilian facilities. Indicators have been formed to assess enemy threats. Qualitative threat assessments were used, using a linguistic variable. To form the necessary defense, the most threatening locations and launch points for enemy strike drones were identified using lexicographical ordering of options.

4. Rationale for creating defense for critical military and civilian facilities from massive attacks by enemy strike drones

Locations of defense means (ADM, EW, AAW, ID),) against attacking actions by enemy strike drones, related to the protection of military facilities (command posts, communications centers, military equipment groups, etc.), as well as dual-purpose infrastructure facilities (bridges, railway stations, warehouses, industrial enterprises, etc.).

When creating a defense potential, it is necessary to take into account the limited possibilities for allocating resources (ADM, EW, AAW, ID), as well as the criticality of objects that need to be protected from enemy drone attacks. Thus, the solution to the task of creating defense to protect military and civilian facilities must be formed in conditions of limited capabilities.

To solve this problem, it is necessary to use indicators, the evaluation of which will allow to rationalizing the necessary defense potential, in the form of a set of means (ADM, EW, AAW, ID) under conditions of limiting their number:

- set (ADM) that is necessary to ensure the protection of the j-th object (MF, CF) – B_j;
- set (EW) that is necessary to ensure the protection of the j-th object (MF, CF) – P_j;
- set (AAW) that is necessary to ensure the protection of the j-th object (MF, CF) – Q_j;
- set (ID) that is necessary to ensure the protection of the j-th object (MF, CF) – S_j.

Where $j=\overline{1,N}$, N – the number of objects (MF, CF) to be protected. To simplify the presentation of the values of the indicators (B_j, P_j, Q_j, S_j), we will use qualitative assessments formed by military experts using the linguistic variable z_{jk}:

$$z_{jk}=\begin{cases}\text{A – minimum value of the k-th indicator is required to provide the j-th object (MF, CF);}\\ \text{B – satisfactory value of the k-th indicator is required to provide the j-th object (MF, CF);}\\ \text{C – large value of the k-th indicator is required to provide the j-th object (MF, CF);}\\ \text{D – very large value of the k-th indicator is required to provide the j-th object (MF, CF).}\end{cases} \quad (6)$$

Depending on the characteristics and criticality of a particular object (MF, CF), we will formulate the priority of indicators (B_j, P_j, Q_j, S_j) for each location (MF, CF), using intelligence regarding the enemy's ability to attack the j-th object (MF, CF). For example, for the jth object (MF, CF) we have the following priority of indicators: B_j, Q_j, P_j, S_j, which means the use of AAW – the highest priority, and the use of ID – the lowest priority. Taking into account the values of the linguistic variable z_{jk}, the protection of the j-th object (MF, CF) can be represented as a tuple of indicator scores, for example: C B A B. Next, we will form a set of means (ADM, EW, AAW, ID) for the protection of objects (MF, CF) in the form of a set of tuples of indicator assessments taking into account their priority.

For example, we have 12 possible objects (MF, CF) that require defense using means (ADM, EW, AAW, ID). The tuples of defense estimates are as follows:

1. C B A B	7. B C A A	
2. B A C B	8. B B A A	
3. C B B C	9. C C B B	(7)
4. D C A A	10. D B A B	
5. C A B B	11. C B C B	
6. D B C B	12. D C C B.	

We organize lexicographically the tuples of estimates of means (ADM, EW, AAW, ID) for creating defense of objects (MF, CF)). Then we will get:

2. B A C B	11. C B C B	
8. B B A A	9. C C B B	
7. B C A A	10. D B A B	(8)
5. C A B B	6. D B C B	
1. C B A B	4. D C A A	
3. C B B C	12. D C C B.	

Thus, the least relevant for the defense of facilities (MF, CF) is the use of means (ADM, EW, AAW, ID) for the options that are at the end of the ordered series of means (ADM, EW, AAW, ID). The most relevant options are at the beginning of the series. Limited opportunities for creating a set of means (ADM, EW, AAW, ID) don't allow the military to create protection for all objects (MF, CF). Therefore (see section 3), it is necessary to reduce the number of objects (MF, CF) for defense by using a restriction in the form of a threshold value of indicators, for example: $\boxed{\text{C B B B}}$. Then we get:

2. B A C B
8. B B A A
7. B C A A
5. C A B B
1. C B A B
$\boxed{\text{C B B B}}$
3. C B B C (9)
11. C B C B
9. C C B B
10. D B A B
6. D B C B
4. D C A A
12. D C C B.

Thus, it is necessary to create defense using means (ADM, EW, AAW, ID) for the following objects (MF, CF):

3. C B B C
11. C B C B
9. C C B B
10. D B A B (10)
6. D B C B
4. D C A A
12. D C C B.

Thus, in this section, the task of substantiating a set of objects (MF, CF) that require protection from massive attacks by enemy strike drones was set and solved. The necessary means (ADM, EW, AAW, ID) have limitations on the creation of their plurality, for the defense of objects (MF, CF). Indicators have been formed that are related to the possibility of allocating resources (ADM, EW, AAW, ID) for each location of protection of facilities (MF, CF) from enemy attacks. To simplify the use of indicators, a linguistic variable with qualitative indicator scores was introduced. The set of object locations (MF, CF) is represented by tuples of qualitative assessments of means (ADM, EW, AAW, ID). A lexicographic ordering of the set of object variants (MF, CF) was carried out. Using the specified threshold values of indicators, objects relevant for defense (MF, CF) that need to be protected in conditions of limited capabilities are identified.

5. Formation of the necessary defense potential of anti-drone means, taking into account limited capabilities

Regular monitoring and reconnaissance of the battlefield allows us to identify the locations and launch sites of enemy strike drones (LLSESD) to carry out offensive actions against military and civilian facilities (MF, CF). With the help of intelligence and military experts, it is possible to assess the enemy's combat potential (P''), as well as possible directions of movement of strike drones to locations (MF, CF). For successful protection of objects (MF, CF), it is necessary to create a defense potential (P'), which must ($P' \geq P''$) to ensure the defense of objects (MF, CF). However, limited opportunities for creating the necessary defense potential, in the form of a set of means (ADM, EW, AAW, ID), do not allow fully fulfilling the conditions ($P' \geq P''$) for all objects (MF, CF). Therefore, a difficult task arises to ensure protection from the attacking actions of enemy strike drones for relevant (critical) facilities (MF, CF). Due to the limitations of defense resources (ADM, EW, AAW, ID), the solution to the task of allocating them for defense (MF, CF) has multiple alternative options. The combinatorial representation of a set of alternative options for the possible composition of defense resources (ADM, EW, AAW, ID) can be combined using

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

a binary counter. The number of options: $K=2^n-1=2^4-1=15$, and the set of options can be represented as:

1. 0001	8. 1000	
2. 0010	9. 1001	
3. 0011	10. 1010	
4. 0100	11. 1011	(11)
5. 0101	12. 1100	
6. 0110	13. 1101	
7. 0111	14. 1110	
	15. 1111.	

Where the first position is related to the use of ADM, the second is related to the use of EW, the third is related to the use of AAW, and the fourth is related to the use of ID. For example, for the sixth option (0110), the composition of the defense potential includes EW and AAW (ADM and ID means aren't used). The selection of the required composition of means for defense will be carried out using the Boolean variable x_{jk}:

$$x_{jk}=\begin{cases}1, \text{ if for the defense}\left(\text{MF, CF}\right)\\ \text{of j-th location the k-th}\\ \text{set of defense means is used}\\ \left(\text{ADM, EW, AAW, ID}\right);\\ 0, \text{ in the other case.}\end{cases} \quad (12)$$

We will use the following indicators to solve the problem of the distribution of defense means:

P_j' – defense potential that must be formed to protect objects (MF, CF) in the j-th location. It is formed using means (ADM, EW, AAW, ID, ...);

P_j'' – the enemy's combat potential, which is formed to carry out an attack with strike drones on the j-th location of objects (MF, CF). It is estimated using intelligence and the opinions of military experts.

Taking into account the Boolean variable x_{jk}, we get:

$$P_j'=\sum_{k=1}^{2^n-1} p_{jk}'x_{jk}\ , \quad (13)$$

where n – the number of types of defense equipment (ADM, EW, AAW, ID, ...).

p_{jk}' – defense potential, which is allocated for the protection of objects (MF, CF) in the j-th location. It is created using the kth composition of defense means (ADM, EW, AAW, ID, ...).

It is necessary that $(P_j'\geq P_j'')$ for all $j=\overline{1,M}$. However, limited possibilities for creating defense for all locations of objects (MF, CF) will lead to the fact that $(P_j'\geq P_j'')$ will not be fulfilled for all objects (MF, CF). Therefore, meeting the requirements $(P_j'\geq P_j'')$ is possible only for the most important (critical) facilities (MF, CF). This leads to the search for a rational distribution of defense means (ADM, EW, AAW, ID, ...) for the protection of a set of objects (MF, CF). We will use the integer (Boolean) programming method to solve the problem. It is necessary to find:

$$\max P',\ P'=\alpha_1\sum_{k=1}^{2^n-1} p_{1k}'x_{1k}+\alpha_2\sum_{k=1}^{2^n-1} p_{2k}'x_{2k}+\ldots+\alpha_M\sum_{k=1}^{2^n-1} p_{Mk}'x_{Mk}, \quad (14)$$

where p_{jk}'– defense potential of the k-th composition of defense means of objects (MF, CF) for the j-th location (assessment by military experts);

M – the number of locations of objects (MF, CF);

α_j – the "weight" of the importance of the j-th object (MF, CF). It is necessary that: $\alpha_1+\alpha_2+\ldots+\alpha_M=1$. The value of the importance of objects (MF, CF) is set by military experts.

When solving the problem, it is necessary to fulfill the conditions regarding the restrictions on the creation of defense potential for each e-th type of means (ADM, EW, AAW, ID, ...).

$$P_e'\leq P_e,\ P_e'=\sum_{j=1}^{M} p_{je}x_{je}\ ,\ \text{for all e},\ e=\overline{1,n}\ , \quad (15)$$

where P_e – restrictions on the e-th type of defense means (ADM, EW, AAW, ID, ...).

Solving the problem, using the integer (Boolean) programming method, depends on the number of options:

- a complete search for possible options, if there aren't many of them;
- targeted search for options with a large number of them, using a modified branch and bounds method;
- a random method of sorting through a very large number of options, which does not allow finding a strict extremum, but makes it possible to improve the value of the indicator (for example, in percentage).

Thus, in this section, the task of substantiating the defense potential of facilities (MF, CF) against massive attacks by enemy strike drones was set and solved. Limited opportunities for allocating defense means, in the form of (ADM, EW, AAW, ID, ...), led to the need for their rational distribution, taking into account the importance (criticality) of objects (MF, CF). The use of the integer (Boolean) programming method, taking into account the importance of the objects (MF, CF) that

need to be defended, made it possible to find a rational solution among possible alternative options for creating defense against massive attacks by enemy strike drones, in conditions of limited capabilities.

6. Multi-agent simulation model for analyzing possible scenarios of massive enemy strike drone attacks

In modern warfare, the situation on the battlefield is changing rapidly. Therefore, it is necessary to conduct a dynamic analysis of actions to create defenses for facilities (MF, CF) from attacking missions of enemy strike drones. Simulation modeling allows, on a given time scale, to analyze possible scenarios of attacking and defensive actions, as well as to assess the possibilities for creating defense of facilities (MF, CF) in conditions of military threats [33]. Therefore, a simulation model was created using the Any Logic agent platform. The multi-agent model allows analyzing the threat of destruction of objects (MF, CF) by enemy strike drones, predicting possible flight routes of drones, and assessing, in time, both the attacking actions of strike drones and the formation of defense means (ADM, EW, AAW, ID). At the same time, it is possible to change the location and launch of the enemy's attack drones, to form different numbers of drones and their combat potential, as well as to evaluate the capabilities of different components of defense equipment (ADM, EW, AAW, ID) in reflecting enemy attacks. This allows for in-depth analysis, over time, of defensive actions and their prediction for various scenarios of massive attacks by enemy strike drones.

The set of agents consists of:

1. The "battlefield map" agent. It is used to specify the locations (LLSESD) of the enemy, as well as the location of objects (MF, CF). On the map, you can set the navigation points of the flight of the enemy's attack drones, form different trajectories and flight routes.

2. The "enemy's location" agent. It is used to fix on the map the navigational coordinates of the location of a number of places (LLSESD) of the enemy.

3. The "locations (MF, CF)" agent. Locations of military facilities and dual infrastructure facilities that can be attacked by enemy strike drones are formed.

4. The "formation of defense potential" agent. Used to assign (in conventional units) the defense potential of means (ADM, EW, AAW, ID) to protect the locations of objects (MF, CF).

5. The "formation of enemy combat potential" agent. The agent is used to determine the combat potential of each enemy location (LLSESD).

6. The "risk of enemy breakthrough" agent. It is given as the probability of enemy breakthrough to the locations of objects (MF, CF). Its value depends on the distance of the attack, as well as the combat potential of enemy and defense means (ratio P′, P′′).

7. The "destroying attack drones" agent. The probability of destroying enemy attack drones is given, taking into account the ratio of defensive and combat potentials (P′, P′′).

8. The "destruction of objects (MF, CF)" agent. The probability of destruction of objects (MF, CF) is given taking into account the ratio of combat and defense potentials (P′, P′′).

9. The "flight route of attack drones" agent. The flight route of a swarm of drones is specified in the form of a sequence of navigation points on the aerial flight map.

10. The "characteristics of a swarm of attack drones" agent. Speed, flight time, etc. are given.

11. The "initialization of the launch of attack drones" agent. The launch of enemy attack drones from each drone launch location is initiated in time.

12. The "interactive modeling control" agent. This agent creates control, in time, of individual simulation modeling agents.

13. The "simulation results" agent. It is used to form the results of simulation modeling:

- flight map with a given set of enemy objects (VO, CO) and locations (LLSESD);
- defense potential for protecting each object (MF, CF) using means (software, electronic warfare, air defense, DP);
- enemy combat potential for each location (MRZUD) of the enemy;
- number of enemy strike drones that reached the targets;
- number of enemy strike drones that were shot down;
- flight routes of a swarm of enemy strike drones; - risks of hitting objects (MF, CF);
- objects that were hit (MF, CF).

Fig. 1 shows the structural diagram of the multi-agent model.

Thus, in this section, a simulation model was created that allows us to study the enemy's attacking actions, in time, using a swarm of strike drones. Possible flight routes of a swarm of strike drones from their locations to the locations of objects (MF, CF) were formed.

The creation of various ratios of the defensive potentials and combat potential of the enemy allows us to assess the success of the breakthrough of enemy strike drones, the possibility of defensive actions to protect objects (MF, CF). The use of various scenarios of combat attacks by enemy strike drones and their display on the map allows analyzing the results of enemy attack missions and defense actions to protect military facilities and dual critical infrastructure facilities.

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

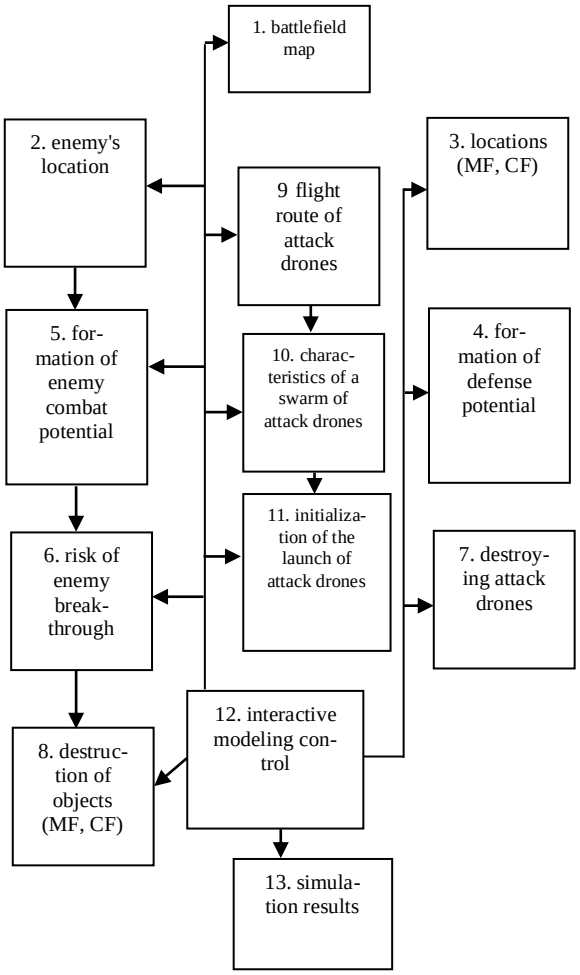

Figure 1. The structural diagram of the multi-agent model

7. An illustrated example of the rational distribution of defense means to protect critical objects from attacks by enemy strike

In section 3, an illustrated example was provided of analyzing possible locations and launches of enemy strike drones (LLESD) with the identification of those that pose a threat to military and civilian facilities that require protection.

In section 4, an illustrated example of the justification of the set of critical objects subject to protection was provided.

In this section, we will consider an illustrated example of the distribution of defense means (ADM, EW, AAW), in conditions of their limited number in relation to objects (MF, CF) (see section 5).

Suppose the military administration has identified three objects that are critical and can be attacked by enemy strike drones. The first object for which defenses need to be created is the dual-purpose logistics center located at location (M1). The second object, in the form of an industrial enterprise that produces current products (strike drones), is located in the location (M2). The third object, in the form of a military command center (in a protected shelter), is located at location (M3).

After analyzing current intelligence data and the enemy's capabilities to conduct offensive actions using strike drones, an assessment was made, on a point scale (0÷10), of the enemy's possible combat potential for conducting a military mission, the goal of which is objects (MF, CF) located in locations (M1, M2, M3):

$$P_{M1}'' = 9 \text{ points}, P_{M2}'' = 4 \text{ points}, P_{M3}'' = 8 \text{ points}.$$

Taking into account the values of the indicators (P_{M1}'', P_{M2}'', P_{M3}''), a priority of places (M1, M2, M3) was formed, in which objects (MF, CF) are located for the creation of defense: M1, M3, M2. When creating defense, it is necessary that (see section 5):

$$P_{M1}' \geq P_{M1}'', P_{M2}' \geq P_{M2}'', P_{M3}' \geq P_{M3}''.$$

Given the limited capabilities in terms of defense capabilities (ADM, EW, AAW), the military was allocated:

$$F_{ADM} = 3 \text{ devices}, F_{EW} = 2 \text{ stations},$$
$$F_{AAW} = 3 \text{ anti-aircraft batteries}.$$

Next, an assessment was made, on a point scale (0÷10), of the defense potential of each type of means:

ADM – 2 points,
EW – 5 points,
AAW – 3 points.

Taking into account the characteristics of each object (MF, CF), as well as the enemy's capabilities for attacking actions using strike drones (see section 3), the following distribution of types of defensive means was created for each location (M1, M2, M3):

1st place: EW, AAW.
2nd place: ADM, AAW.
3rd place: ADM, EW.

For each type of defense means, taking into account the allocated quantity, using combinatorial calculations, a complete set of options for distributing them by location (M1, M2, M3) in which the objects (MF, CF) are located was formed. So, for the ADM we have the following possible distribution options by location (M2, M3), which are presented in Table 1.

Table 1

Variants of ADM distribution

№	M2	M3
1.1	0	3
1.2	1	2
1.3	2	1
1.4	3	0

For EW, we have the following distribution options by location (M1, M3), which is presented in Table 2.

Table 2

Distribution options for EW

№	M1	M3
2.1	0	2
2.2	1	1
3.3	2	0

For AAW, we have the following distribution options by location (M1, M2), which are presented in Table 3.

Table 3

Variants of AAW distribution

№	M1	M2
3.1	0	3
3.2	1	2
3.3	2	1
3.4	3	0

Next, for each location (M1, M2, M3) a complete set of distribution options (ADM, EW, AAW) with estimates of possible defense potential was created using exhaustive search (see Section 5).

For the first location (M1), where the logistics center is located, we have the following options with estimates of possible defense potential (Table 4).

For the second location (M2), where the industrial enterprise is located, Table 5 was formed.

For the third location (M3), in which the military control center is located, Table 6 was formed.

After analyzing Tables 4, 5, 6, unnecessary options that didn't meet the requirements were discarded:

$$P_{M1}' \geq P_{M1}'' = 9,\ P_{M2}' \geq P_{M2}'' = 4,\ P_{M3}' \geq P_{M3}'' = 8.$$

Therefore, for location (M1), we produce the following reduced number of options for the distribution of defense means (Table 4):

4, 7, 8, 9, 10, 11, 12.

For the location (M2) we obtain the following reduced multiple of options (Table 5):

1, 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16.

Table 4

Assessment of defense potential for (M1)

	Variants		Calculation of defense potential	Defense potential
№	EW	AAW		
1	2.1	3.1	0x5+0x3	0
2	2.1	3.2	0x5+1x3	3
3	2.1	3.3	0x5+2x3	6
4	2.1	3.4	0x5+3x3	9
5	2.2	3.1	1x5+0x3	5
6	2.2	3.2	1x5+1x3	8
7	2.2	3.3	1x5+2x3	11
8	2.2	3.4	1x5+3x3	14
9	2.3	3.1	2x5+0x3	10
10	2.3	3.2	2x5+1x3	13
11	2.3	3.3	2x5+2x3	16
12	2.3	3.4	2x5+3x3	19

Table 5

Assessment of defense potential for (M2)

	Variants		Calculation of defense potential	Defense potential
№	ADM	AAW		
1	1.1	3.1	0x2+3x3	9
2	1.1	3.2	0x2+2x3	6
3	1.1	3.3	0x2+1x3	3
4	1.1	3.4	0x2+0x3	0
5	1.2	3.1	1x2+3x3	11
6	1.2	3.2	1x2+2x3	8
7	1.2	3.3	1x2+1x3	5
8	1.2	3.4	1x2+0x3	2
9	1.3	3.1	2x2+3x3	13
10	1.3	3.2	2x2+2x3	10
11	1.3	3.3	2x2+1x3	7
12	1.3	3.4	2x2+0x3	4
13	1.4	3.1	3x2+3x3	15
14	1.4	3.2	3x2+2x3	12
15	1.4	3.3	3x2+1x3	9
16	1.4	3.4	3x2+0x3	6

Table 6

Assessment of defense potential for (M3)

	Variants		Calculation of defense potential	Defense potential
№	ADM	EW		
1	1.1	2.1	3x2+2x5	16
2	1.1	2.2	3x2+1x5	11
3	1.1	2.3	3x2+0x5	6
4	1.2	2.4	2x2+2x5	14
5	1.2	2.1	2x2+1x5	9
6	1.2	2.2	2x2+0x5	4
7	1.3	2.3	1x2+2x5	12
8	1.3	2.4	1x2+1x5	7
9	1.3	2.1	1x2+0x5	2
10	1.4	2.2	0x2+2x5	10
11	1.4	2.3	0x2+1x5	5
12	1.4	2.4	0x2+0x5	0

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

For the location (M3) we obtain the following reduced set of options (Table 6):

1, 2, 4, 5, 7, 10.

Next, it is necessary to take into account the allocated number of defense assets for each type ($F_{ADM} = 3$, $F_{EW} = 2$, $F_{AAW} = 3$).

Therefore, for the first, most priority for defense, location (M1), where the logistics center is located, 7 variants were used (Table 4), in which:

EW – 1, AAW – 2.

Defense potential for the 7th variant $P_{M1}'=11$. The condition is met: $P_{M1}' \geq P_{M1}''$ (11 > 9).

For the second location (M2), where the industrial enterprise is located, the 7th variant was used (Table 5), for which:

ADM – 1, AAW – 1.

Defense potential for the 7 th variant $P_{M2}' = 5$. The condition is met: $P_{M2}' \geq P_{M2}''$ (5 > 4).

For the third location (M3), in which the military control center is located, the 5 th variant was used (Table 6), in which the following are located:

ADM – 2, EW – 1.

Defense potential for the 5 th variant $P_{M3}' = 9$. The condition is met: $P_{M3}' \geq P_{M3}''$ (9 > 8).

Thus, this section presents an illustrated example of the use of the proposed approach to justify the creation of a defense potential for the protection of objects: a logistics center (dual purpose), an industrial enterprise, a military control center (in a protected shelter). Due to restrictions on the allocation of defense means (ADM, EW, AAW) to the military, it became necessary to create and analyze a set of possible options for distributing defense means in relation to the locations of military and civilian facilities. Possible variants were analyzed and the optimal one was chosen, which satisfies the conditions of limited opportunities for creating a defensive potential, for actively countering the attacking missions of the enemy's attack drones.

8. Discussion

A systematic presentation of the sequence of military logistical actions for the formation of defensive means against massive attacks by enemy strike drones has been created. The circumstances on the battlefield have been analyzed to identify the most threatening locations and launch sites for enemy strike drones. The actual, most threatening enemy locations for attacks that can damage military and civilian facilities have been substantiated. An analysis was conducted to assess the enemy's possible combat potential, in the form of a value (P″). Critical military and civilian facilities that could be primarily attacked by enemy strike drones were analyzed. The necessary defense potential (P′) was identified. For successful defense of military and civilian facilities, it is necessary that (P′≥P″). However, due to the limited number of defense means, difficulties arise in creating a full-fledged defense of military and civilian facilities. Therefore, the problem of rational distribution of defense resources arose and was solved, in the form of: ADM, EW, AAW, ID from attacking enemy strike drones, in order to ensure the protection of the most critical facilities. A simulation was conducted, on a given time scale, of the attacking actions of enemy strike drones using the Any Logic platform. An illustrated example is provided that clearly demonstrates the effectiveness of the proposed approach for creating a defense potential using ADM (three devices), EW (2 stations), AAW (3 anti-aircraft batteries) to protect critical facilities: a dual-purpose logistics center, an industrial enterprise that produces attack drones, and a military control center (in a protected shelter).

The following research methodology is proposed:

- systematic presentation of the sequence of defensive actions to protect military and civilian facilities from attacks by enemy strike drones;
- analysis of the locations and launches of enemy strike drones to identify the most threatening ones, in relation to military and civilian facilities;
- justification of the current locations of military and civilian facilities for their protection;
- formation of the necessary defense potential for the protection of military and civilian facilities, in conditions of limited opportunities for the full use of defense means;
- modeling scenarios for conducting offensive actions by enemy strike drones and defensive actions for the protection of critical military and civilian infrastructure facilities.

When solving problems with multiple options, the dimensionality problem is taken into account as follows:

- with a relatively small number of options, a complete search or lexicographic ordering of options was used (using both quantitative and qualitative assessments) (1) – (11);
- with a large number of options, integer (Boolean) programming or a random method (12) – (15) can be used;
- in the example of the article, a search was conducted for the distribution of defense assets (ADM, EW,

AAW) using indicators of the enemy's combat potential and the defense potential of the defense. The optimal option was found (7, defense potential in points - 12). This is 75% of the maximum (1 option, defense potential -16 points) and improves our defense capabilities, in conditions of limited resources.

The developed modeling tool allows you to optimize the implementation of defensive actions and minimize the number of resources for the defense of objects (MF, CF).

The relevance of the proposed approach is related to the need for scientific substantiation of the defense potential of protection against the attacking actions of enemy strike drones, in conditions of limited capabilities.

The developed set of models is aimed at planning defensive actions to protect military and civilian facilities from massive attacks by enemy strike drones. This allows us to conclude that the proposed approach is timely and effective for creating effective defense against enemy attack drone missions.

The effectiveness of the proposed approach is associated with a systematic combination of methods for qualitative and quantitative assessment of options for planning defensive actions against attacking waves of enemy strike drones, in conditions of limited opportunities for allocating resources to protect critical military and civilian facilities.

Future research will focus on improving applied information technology for modeling defensive military operations to protect military facilities and dual-purpose infrastructure from massive swarm attacks by enemy strike drones.

9. Conclusions

The conducted research allows you to model and plan defensive actions to protect military and civilian facilities from massive attacks by enemy strike drones, using ADM, EW, AAW and ID, namely:

- to form a logistical sequence of defensive actions to protect military facilities and critical infrastructure facilities;

- to analyze the threatening locations and launches of enemy strike drones;

- to substantiate the current defense locations of military and civilian facilities, which, first of all, need to be protected from swarm attacks by enemy strike drones;

- to form a defensive potential as part of anti-drone means to reflect attacking missions by enemy strike drones;

- to analyze various attack scenarios and flight routes of a swarm of strike drones to plan defensive actions to protect critical facilities.

The scientific novelty of the proposed approach lies in the scientific substantiation of defensive actions to protect military and civilian facilities from massive attacks by enemy strike drones based on the use of the developed complex of original and new mathematical and simulation models. Thus, we can make the main conclusion (the main contribution) regarding the conducted research:

The proposed set of models allows to substantiate the logistical sequence of defensive actions to create an active shield of protection, in the form of anti-drone means, to protect military and civilian facilities from massive attacks by enemy strike drones. This will ensure the effectiveness of the use of defensive means against enemy attacking actions, in conditions of limited capabilities, minimizing military resources and reducing time for planning countermeasures against the enemy.

Contribution of authors: systematic analysis of military operations to create defense against massive attacks by enemy strike drones – **Oleg Fedorovich**; analysis and justification of the defense of military and civilian facilities from attacks by enemy strike drones – **Olga Malyeyeva;** selection of critical objects for protection **– Andrii Humennyi;** formation of the necessary defense potential for protection – **Oleksandr Leshchenko**; flight simulation of attack drones – **Yuliia Leshchenko;** simulation of enemy attack scenarios – **Ganna Pliekhova**.

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. Henriksen D., & Bronk, J. *The Air War in Ukraine. The First Year of Conflict*. 2024 Pub. Location

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

London, Imprint Routledge. 252 p. DOI: 10.4324/9781003454120.

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. Anishchukov, I. V., Meder, O. V., & Nesteruk, V. L. *Metodychni rekomendatsiyi z planuvannya ta orhanizatsiyi boyu za standartamy NATO (shtab bryhady (batal'yonu) ta yim rivnykh* [Methodological recommendations for planning and organizing combat according to NATO standards (brigade (battalion) headquarters and their equivalents]. Kyyiv, Navchal'nyy tsentr pidhotovky pidrozdiliv Mizhnarodnoho tsentru myrotvorchosti ta bezpeky, 2020. 136 p. Available at: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/ВП-75-001103.01-Планування-та-організація-бою-за-стандартами-НАТО.pdf (accsessed 20.05.2025). (in Ukrainian).

4. Kodam, S., Bharathgoud, N., & Ramachandran, B. A review on smart wearable devices for soldier safety during battlefield using WSN technology. *Materials Today: Proceedings*, 2020, vol. 33, part 7, pp. 4578-4585. DOI: 10.1016/j.matpr.2020.08.191.

5. Čisar, P., Pinter, R., Čisar S. M., & Gligorijević, M. Principles of Anti-Drone Defense. *11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)*, Mariehamn, Finland, 2020, pp. 000019-000026, DOI: 10.1109/CogInfoCom50765.2020.9237841.

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, vol. 17, no. 2, pp 455-461. DOI: 10.12716/1001.17.02.23.

7. Pytel, M., & Cieśla, M. Use of Territorial Defense Forces (TDF) in combat operations. *Scientific Journal of the Military University of Land Forces*, 2021, vol. 199, no. 1, article no. 15, pp. 61-72. DOI: 10.5604/01.3001.0014.8110.

8. Constantinescu, M. Challenges of defining a country's military power. *Journal of Defense Resources Management (JoDRM)*, 2020, vol. 11, iss. 2 pp. 32-39. Available at: https://www.ceeol.com/search/article-detail?id=914137. (accsessed 20.05.2025).

9. 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.

10. Yu, A., Kolotylo, I., Hashim, H. A., & Eltoukhy, A. E. E. Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics: A Survey. *In IEEE Access*, 2025, vol. 13, pp. 68660-68681, DOI: 10.1109/ACCESS.2025.3561068.

11. Calcara, A., Gilli, A., Gilli, M., Marchetti, R., & Zaccagnini I. Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare. *International Security*, 2022, vol. 46, iss. 4, pp. 130-171. DOI: 10.1162/isec_a_00431.

12. 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.

13. Abdelkader, M., Güler, S., Jaleel, H., & Shamma, J. S. Aerial swarms: Recent applications and challenges. *Current robotics reports*, 2021, no. 2, pp. 309-320. DOI: 10.1007/s43154-021-00063-4.

14. 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.

15. Movchan, K. O. Systemy klasyfikatsiyi bezpilotnykh lital'nykh aparativ ta yikh zastosuvannya v riznykh haluzyakh [Classification systems for unmanned aerial vehicles and their application in various industries]. *Haluzeve mashynobuduvannya – Industrial Mechanical Engineering*, 2024, vol. 35 (74), no. 6, pp. 1-7. DOI: 10.32782/2663-5941/2024.6.1/01. (in Ukrainian).

16. Lee, M., Choi, M., Yang, T., Kim, Ji., Kim, Ja., & Kwon O. A Study on the Advancement of Intelligent Military Drones: Focusing on Reconnaissance Operations. *IEEE Access*, 2024, vol. 12, pp. 55964-55975. DOI: 10.1109/ACCESS.2024.3390035.

17. Zibetti, G. R., Wickboldt, J. A., & Pignaton de Freitas, E. Context-aware environment monitoring to support LPWAN-based battlefield applications. *Computer Communications*, 2022, vol. 189, pp. 18-27. DOI: 10.1016/j.comcom.2022.02.020.

18. Mao, T. -J., Zhang, D., Niu, Y., Yu, M., Liang, X., & He, M. The Determination Method of Battlefield Monitoring Interval Period Based on the Complicatedness of Situation Changes. *IEEE Access*, 2021, vol. 9, pp. 165947-165955. DOI: 10.1109/ACCESS.2021.3135040.

19. Hrnčiar, M., Kompan, J., & Nohel, J. The future of the battlefield: Technology-driven predictions in the land domain. *Revista Científica General José María Córdova*, 2025, vol. 23, no. 49, pp. 277-296. DOI: 10.21830/19006586.1323

20. 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, iss. 3, article no. 65. DOI: 10.3390/drones6030065.

21. Najgebauer, A.: Consideration of electronic warfare in the assessment and development of the operational capabilities of the armed forces. *IET Radar Sonar & Navigation*, 2024, vol. 18, iss. 11, pp. 2199–2211. DOI: 10.1049/rsn2.12629.

22. Li, N., Su, Z., Ling, H., Karatas, M., & Zheng, Y. Optimization of Air Defense System Deployment Against Reconnaissance Drone Swarms. *Complex System Modeling and Simulation*, 2023, vol. 3, no. 2, pp. 102-117. DOI: 10.23919/CSMS.2023.0003.

23. Park, S., Kim, H. T., Lee, S., Joo, H., & Kim, H. Survey on Anti-Drone Systems: Components, Designs, and Challenges. *In IEEE Access*, 2021, vol. 9, pp. 42635-42659. DOI: 10.1109/ACCESS.2021.3065926.

24. Opirskyy, I., & Bybyk, R. Doslidzhennya suchasnykh metodiv reb ta metodiv i zasobiv yiyi protydiyi [Research on modern methods of Electronic Warfare (EW) and methods and means of its counteraction]. *Bezpeka informatsiyi – Ukrainian Scientific Journal of Information Security*, 2023, vol. 29, iss. 2, pp. 88-97. DOI: 10.18372/2225-5036.29.17873 (in Ukrainian)

25. Najgebauer, A. Consideration of electronic warfare in the assessment and development of the operational capabilities of the armed forces. *IET Radar, Sonar & Navigation*, 2024, vol. 18, iss. 11, pp. 2199-2211. DOI: 10.1049/rsn2.12629.

26. Choi, S., Kwon, O.-J., Oh, H., & Shin, D. Method for Effectiveness Assessment of Electronic Warfare Systems in Cyberspace. *Symmetry*, 2020, vol. 12, iss. 12, article no. 2107. DOI: 10.3390/sym12122107.

27. 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, vol. 9, iss. 12, article no. 747. DOI: 10.3390/aerospace9120747.

28. Ricardo, J. A., Giacomossi, L., Trentin, J. F. S., Brancalion, J. F. B., Maximo, M. R. O. A., & Santos, D. A. Cooperative Threat Engagement Using Drone Swarms. *IEEE Access*, 2023, vol. 11, pp. 9529-9546. DOI: 10.1109/ACCESS.2023.3239817.

29. Trishch, R., Cherniak, O., Zdenek, D., & Petraskevicius, V. Assessment of the occupational health and safety management system by qualimetric methods. *Engineering Management in Production and Services*, 2024, vol. 16, iss. 2. pp. 118-127. DOI: 10.2478/emj-2024-0017.

30. Cherniak, O., Trishch, R., Ginevičius, R., Nechuiviter, O., & Burdeina, V. Methodology for assessing the processes of the occupational safety management system using functional dependencies. *Integrated Computer Technologies in Mechanical Engineering – 2023 (ICTM 2023)*. Lecture Notes in Networks and Systems, 996. Springer, Cham, 2024, pp. 3-13. DOI: 10.1007/978-3-031-60549-9_1.

31. Dawidczyk, A. *National Defensive and Defense Strategies. Selected Planning Problems*. Scientific Reports of Fire University ZN SGSP, 2020, vol. 76, pp. 69-91. DOI: 10.5604/01.3001.0014.5979.

32. 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. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2023, no. 4, pp. 209-220. DOI: 10.32620/reks.2023.4.1

33. Fedorovich, O., Krytskyi, D., Lukhanin, M., Prokhorov, O., & Leshchenko, Yu. Modeling of strike drone missions for conducting wave attacks in conditions of enemy anti-drone actions. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2025, no. 1, pp. 29-43. DOI: 10.32620/reks.2025.1.02

Received 04.05.2025, Accepted 25.08.2025

МОДЕЛЮВАННЯ ОБОРОННИХ ДІЙ ЩОДО ЗАХИСТУ ВІЙСЬКОВИХ ТА ЦИВІЛЬНИХ ОБ'ЄКТІВ ВІД МАСОВАНИХ ХВИЛЬОВИХ АТАК УДАРНИХ ДРОНІВ ПРОТИВНИКА

О. Є. Федорович, О. В. Малєєва, А. М. Гуменний, О. Б. Лещенко, Ю. О. Лещенко, Г. А. Плєхова

Умови сучасної гібридної війни вимагають створення необхідного оборонного потенціалу для захисту військових об'єктів та критичної інфраструктури від масованих атак ударних дронів противника. Особливістю відображення повітряних атак дронів є використання різноманітного арсеналу захисних засобів (протидронові засоби, РЕБ, ППО, дрони-перехоплювачі, тощо). Тому, **актуально** проведення дослідження щодо моделювання оборонних дій та планування захисту військових та цивільних об'єктів від атакуючих місій ударних дронів противника. **Предметом** дослідження, в публікації, є математичні та імітаційна модель, які використовуються для планування захисту військових та цивільних об'єктів від ройових атак ударних дронів противника. **Метою** дослідження є моделювання щодо планування оборонних дій від повітряних атак противника, в умовах обмежених можливостей, що забезпечить раціональне використання військових ресурсів. **Завдання**, які необхідно вирішити: аналіз послідовності оборонних дій; проаналізувати найбільш загрозливі місця формування та запуску ударних дронів противника; обґрунтувати створення оборони критичних військових та цивільних об'єктів; створення необхідного оборонного потенціалу для захисту критич-

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

них військових та цивільних об'єктів; промоделювати можливі сценарії запуску та руху ударних дронів противника; продемонструвати на ілюстрованому прикладі доцільність та ефективність запропонованого підходу. Використані математичні **методи та моделі**: системний аналіз оборонних протидронових дій; якісне оцінювання варіантів оборонних дій за допомогою лінгвістичних змінних; лексикографічне впорядковування варіантів для виділення актуальних місць щодо захисту військових та цивільних об'єктів; метод цілочисельного (булевого) програмування для обґрунтування оборонного потенціалу захисту, в умовах обмежених можливостей; мультиагентне моделювання для аналізу та прогнозування можливих сценаріїв атакуючої місії противника з використанням ударних дронів. Отримано наступні **результати**: запропоновано системне представлення щодо планування оборонних дій від масованих атак ударних дронів противника; обґрунтовані найбільш загрозливі місця формування та запуску рою ударних дронів противника; виділені актуальні місця розташування протидронових засобів для охорони військових об'єктів та об'єктів подвійної інфраструктури; створено необхідний оборонний потенціал для захисту від повітряних атак в умовах обмежених можливостей; розроблена мультиагентна імітаційна модель для аналізу та прогнозування можливих сценаріїв запуску та польоту ударних дронів противника до місць розташування критичних військових та цивільних об'єктів. **Висновки.** Результати проведеного дослідження дозволяють обґрунтувати та планувати оборонні протидронові дії щодо захисту військових об'єктів та об'єктів інфраструктури подвійного призначення. **Наукова новизна** запропонованого підходу полягає в науковому обґрунтуванні оборонних дій щодо захисту військових та цивільних об'єктів від масованих атак ударних дронів противника на основі використання розробленого комплексу оригінальних та нових математичних та імітаційної моделей.

Ключові слова: протидроновий захист; обґрунтування загрозливих місць запуску ударних дронів противника; захист військових та цивільних об'єктів; оптимізація оборонного потенціалу захисту від ударних дронів; лінгвістичні змінні для якісних оцінок експертів; лексикографічне впорядковування варіантів; мультиагентне імітаційне моделювання атак ударних дронів.

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

Малєєва Ольга Володимирівна – д-р техн. наук, проф., проф. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Гуменний Андрій Михайлович – канд. техн. наук, доц., проректор з НПР, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Лещенко Олександр Борисович – канд. техн. наук, проф. ХАІ, проф. каф. комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

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

Плєхова Ганна Анатоліївна – канд. техн. наук, доц., зав. каф. комп'ютерних наук та інформаційних систем, Харківський національний автомобільно-дорожній університет, 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.

Olga Malyeyeva – Doctor of Technical Sciences, Professor, Professor of Computer Science and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: o.malyeyeva@khai.edu; ORCID: 0000-0002-9336-4182.

Andrii Humennyi – Candidate of Technical Sciences, Associate Professor, Vice-Rector for Research and Teaching, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: a.gumennyy@khai.edu, ORCID: 0000-0003-1020-6304, Scopus Author ID: 57219051542.

Oleksandr Leshchenko – Candidate of Technical Science, Professor, Professor at the Department of Computer Science and Information Technology, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine, e-mail: o.leshchenko@khai.edu, ORCID: 0000-0001-9405-4904.

Yuliia Leshchenko – Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Sciences and Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: j.leshhenko@khai.edu, ORCID: 0000-0001-9232-697X.

Ganna Pliekhova – Candidate of Technical Sciences, Associate Professor, Head of the Department of Computer Science and Information Systems, Kharkiv National Automobile and Highway University, Kharkiv, Ukraine, e-mail: plehovaanna11@gmail.com, ORCID: 0000-0002-6912-6520.