UDC 351.862:355.45

Ye. Briukhno **V. Synytskyi**

ORGANIZATIONAL AND MANAGEMENT MECHANISMS FOR INCREASING THE EFFICIENCY OF ACTIONS OF UNITS OF THE NATIONAL GUARD OF UKRAINE IN ENSURING STATE SECURITY IN THE CONDITIONS OF MODERN MILITARY HYBRID THREATS

The article discusses organizational and management mechanisms for improving the effectiveness of the actions of the National Guard of Ukraine in the context of ensuring state security in the context of modern military-hybrid threats. The main tasks of the NGU as a component of the security and defense sector are analyzed, and key factors influencing the combat capability and readiness of units to perform various types of operations (combat, stabilization, security, anti-terrorist) are identified. Considerable attention is paid to the problems of existing organizational and personnel structures and management systems that need to be modernized in the context of dynamic changes on the battlefield, the widespread use of high-precision weapons, unmanned aerial vehicles, radio-electronic security systems, sabotage groups, and cyber threats from the enemy. A set of mechanisms has been developed to improve management, optimize organizational structure, reform personnel policy, enhance technological capabilities, and develop interagency cooperation. A model of a modular structure of units and an algorithm for rapid response to threats.

Keywords: *national security, National Guard of Ukraine, organizational and management mechanisms, combat operations, hybrid threats, organizational and staffing structure.*

Statement of the problem. In the current conditions of full-scale aggression against Ukraine, the issue of ensuring state security is of critical importance. The security and defense sector is under constant pressure, which requires functional adaptation of law enforcement agencies, in particular the National Guard of Ukraine (NGU). Currently, the NGU performs a wide range of duties, from participating in combat operations on the front lines to ensuring public order, protecting strategic facilities, and supporting humanitarian operations and counter-sabotage measures.

The escalation of hybrid military threats, including the widespread use of UAVs, electronic warfare, high-precision weapons, cyberattacks, and sabotage groups, calls for a fundamental review of the current mechanisms for managing NGU units. Key problems include: low flexibility of organizational and staffing structures, excessive centralization of management, insufficient level of digitalization, shortage of specialists in critical professions (UAV operators, electronic warfare specialists, intelligence analysts, C2 officers), as well as limited interagency synchronization [1–4].

In this context, there is a need to develop modern, adaptive, technologically equipped, and personnel-balanced organizational and management mechanisms that will ensure the combat resilience of the NGU units and their ability to operate effectively in a rapidly changing operational environment.

Analysis of recent research and publications. Contributions to the development of mechanisms for state management of the actions of the National Guard of Ukraine in the context of modern military-hybrid threats have been made by such scholars as S. Belay, G. Drobakha, V. Yemanov, O. Iokhov, V. Lisitsin, O. Oleshchenko, E. Smirnov, K. Sporyshev, V. Tkachenko, and others. In particular, the works of S. Belay, V. Yemanov, and K. Sporyshev describe the mechanisms of state management for improving the effectiveness of the actions of the National Guard units in the context of modern threats to state security. Scientists G. Drobakha, O. Iokhov, V. Lisitsyn, O. Oleshchenko, E. Smirnov, and V. Tkachenko examined the fundamentals of the system for managing the actions of the National

Guard units and the mechanisms of state management of the security and defense forces of Ukraine during the performance of their official combat tasks.

The purpose of the article is to identify and justify organizational and management mechanisms that contribute to improving the effectiveness of the National Guard of Ukraine in ensuring state security, as well as to develop practical models for transforming the organizational and staffing structure, management, and personnel policy of the National Guard of Ukraine.

Summary of the main material. The concept of state security encompasses the protection of sovereignty, territorial integrity, political stability, the effective functioning of state institutions, and the inviolability of critical infrastructure. The National Guard occupies a special place in the security system, as it performs both military and law enforcement tasks. The National Guard operates in three main areas: combat, providing defense in designated areas; stabilization, maintaining order in frontline areas; and law enforcement, ensuring the safety of citizens and critical infrastructure.

Such multifunctionality requires a special organizational model – flexible, mobile, high-tech, and balanced in terms of personnel.

Key contemporary threats to national security include the widespread use of various types of UAVs; high-precision artillery and missile strikes; electronic warfare, which complicates communication; sabotage and reconnaissance groups and terrorist attacks; cyberattacks and information and psychological influence; disruption of critical infrastructure [5].

This significantly changes the nature of combat operations and stabilization operations, necessitating the improvement of the management and training of NGU units.

In the current context of the transformation of the national security system, the organizational and management mechanisms of the National Guard of Ukraine are under considerable strain due to the multifunctionality of tasks, changes in the nature of combat operations, the need for synchronization with other components of the security and defense sector, and the rapid evolution of technology. A comprehensive analysis of existing management mechanisms makes it possible to identify structural, functional, and personnel factors that limit the effectiveness of NGU units, as well as to identify potential areas for improvement.

The NGU command system has historically been based on a hierarchical, predominantly centralized approach that ensures vertical subordination and control. This model is effective in law enforcement, public order maintenance, and facility protection, but has limitations in high-risk.

Among the key problems, the following should be noted.

1. Centralization of decision-making. Many tactical decisions are approved at the brigade or operational command level, which leads to wasted time and reduced tactical flexibility. In combat conditions, decisions must be made at the platoon or company level within minutes.

2. Insufficient automated control systems (ACS) [5]. The current control model relies heavily on voice radio communication, which causes delays in command transmission, risk of information loss, increased vulnerability to enemy electronic warfare, and insufficient synchronization between units.

3. Fragmented information integration [5, 6]. NGU units often operate separately from the information flows of the Armed Forces of Ukraine or the Security Service of Ukraine. This limits the acquisition of intelligence data, the coordination of fire support, and the ability to conduct complex operations.

4. Unregulated rapid response algorithms. In some cases, commanders are forced to develop "improvised" response plans that are not documented, which complicates planning and preparation.

The typical organizational and staffing structure of the NGU units is geared toward the mixed performance of law enforcement and military tasks. This creates a number of systemic limitations.

1. The structure does not meet the requirements of multi-domain operations. Modern warfare determines the important role of UAVs (reconnaissance, correction, strike functions), mobile fire groups, electronic warfare means, and sensor reconnaissance systems.

Many NGU units do not have full-fledged aerial reconnaissance groups, engineering and sapper modules, cyber defense and electronic warfare units, or analytical centers for data collection. This creates dependence on third-party structures (the Armed Forces of Ukraine, volunteer groups, volunteer drone operators).

2. Excessive number of "universal" positions. Historically, the NGU has performed many internal security tasks, so a significant part of its units have a universal structure. However, universal companies lose their effectiveness in specific combat tasks.

3. Limited maneuverability. The current structure does not always allow for the rapid formation of modular tactical groups such as: recon-strike; recon-EW; infantry-UAV; stabilization-CIMIC. The restructuring of units for specific tasks often takes place "manually", which is time-consuming.

The NGU personnel system faces a number of critical challenges.

1. Shortage of specialists in high-tech areas: UAV operators (tactical and operational levels); electronic warfare specialists; intelligence analysts; C2 officers; signalers; tactical medicine instructors. The main reasons for the shortage are the lengthy and complex training, the high "cost" of specialists on the front lines, and the lack of incentives to retain personnel.

2. Training programs that don't meet modern requirements: lack of systematic integration of UAVs and electronic warfare in training cycles, not enough simulators and simulations, focus on outdated standards for training law enforcement units, not enough adaptation to real combat experience.

3. Unclear mechanisms for rotation and preservation of experience. In many units, rotations are irregular, there are no mechanisms for monitoring combat fatigue, and the combat experience of individual fighters is lost after transfer or discharge. There is a lack of institutional memory – a system of proven, unified databases of lessons and case studies.

Conducting a modern military operation requires full integration of forces, but interagency cooperation (National Guard–Armed Forces–Security Service–Ministry of Internal Affairs–State Emergency Service) has certain limitations.

1. Lack of a unified information platform. Each agency has its own communication systems, which reduces the speed of data exchange, the accuracy of coordination of operations, and the possibility of joint decisions.

2. Fragmentation of intelligence flows. The NGU does not always receive real-time operational intelligence from the Armed Forces or the Security Service, which is critical when performing counter-sabotage or assault tasks.

3. Insufficient joint training. Some regions do not have permanent training centers where units from different structures could practice joint combat operations, assault operations, stabilization measures, and infrastructure protection.

The analysis allows us to identify key structural problems, in particular:

1) organizational – the structure of departments is not adapted to multi-domain operations;

2) managerial – the centralized C2 model slows down response times;

3) technological – low level of digitization and sensor integration;

4) personnel – lack of specialists and a system for transferring experience;

5) interdepartmental – insufficient synchronization with other law enforcement agencies.

All this reduces the effectiveness of the NGU's combat and stabilization operations, increases decision-making time, and reduces adaptability to new threats.

Improving the effectiveness of the National Guard of Ukraine in the context of modern hybrid military threats is only possible through comprehensive modernization of the organizational and management system. Changes should cover the structure of units, command and control processes, personnel policy, technological equipment, and interagency cooperation. Below is a detailed set of such mechanisms, developed on the basis of an analysis of the experience of the Armed Forces of Ukraine, the National Guard of Ukraine, and the world's leading armies.

The organizational and staffing structure is the foundation of the combat readiness and effectiveness of the NGU units. Its optimization should be carried out in accordance with the principles of modularity, functionality, adaptability to the task, minimal bureaucracy, and support for digital integration.

It is proposed to form standard modules that can be quickly combined for a specific operation.

Recon module:

– reconnaissance groups;

– UAV units;

– visual, signal, and radio reconnaissance group.

Strike module:

– assault group;

– mobile fire group;

– anti-tank missile systems/mortar support;

– FPV strike UAVs.

Support module:
– medical evacuation (Medevac);
– engineering and sapper group;
– logistics;
– repair and maintenance group.

Such modules enable flexible formation of units, minimization of time spent on planning, standardization of interaction between groups, and reduction of irrational elements of the staff.

Based on an analysis of combat experience, the NGU units should systematically include: tactical UAV batteries, electronic warfare and UAV countermeasure companies, operational information analysis centers, cyber defense and C2 communications nodes, data processing and modeling centers. This will enable the unit to achieve autonomy and reduce its dependence on external structures.

It is necessary to reduce the proportion of so-called "universal law enforcement" positions and increase the proportion of UAV operators, reconnaissance specialists, electronic warfare specialists, C2 specialists, tactical medics, sapper engineers, and analysts. This will form a more effective core of the combat unit.

Modern combat conditions require the creation of a management system that ensures rapid decision-making, real-time access to information, resistance to electronic warfare and cyberattacks, and integration into the joint information space of the Armed Forces, National Guard, and Security Service of Ukraine.

Increasing the autonomy of platoons and assault groups reduces decision-making time, dependence on higher headquarters, and the risk of losing communication.

The delegation mechanism should include standardized operating procedures (SOPs), battle cards, and instructions in case of loss of communication.

In the field of digitalization of management, it is necessary to introduce ACS, digital maps with integrated intelligence data, secure data transmission channels (mesh network), and analytical dashboards for commanders. This makes management more accurate and less dependent on the human factor.

The command and control system must have backup C2 systems: mobile command posts, backup communication channels (Starlink, low-frequency communication, fiber optic lines), and autonomous C2 modules in case the main command post is lost.

The personnel unit is critical to ensuring the continuity of combat operations. Modern warfare requires a new approach to personnel work. Today, a system for the rapid training and certification of specialists has already been partially created. According to the authors, training should be modular in nature, using simulation trainers and combat cases, and should include analysis of real operations and standardized certification.

To conduct modern combat operations, it is necessary to establish a Combat Knowledge System. It is proposed to introduce a unified After Action Review database, a video archive of tactical operations, mandatory documentation of "lessons learned" after each battle, and analysis centers within brigades.

In a hybrid war, no structure can act in isolation. Interagency cooperation needs to be deepened by creating joint operational centers. At the regional and operational command levels, it is necessary to create NGU–ZSU–SBU–MVS–DSNS centers with a unified information field and coordinated staff planning; to unify protocols of action, namely to approve unified response standards, information transfer procedures, common communication algorithms, and target designation standards. Possible measures include: creating a joint training system; conducting regular training such as Urban Shield, Border Shield, and Hybrid Defense; training in mixed groups; and training on how to respond to attacks on critical infrastructure.

The proposed set of mechanisms – organizational, managerial, personnel, technological, and interagency – forms the basis for the systematic modernization of the NGU and increases its effectiveness in ensuring national security. Its implementation will contribute to the formation of adaptive, technologically equipped, personnel-stable, and effective combat units capable of operating in a multi-domain war environment.

The proposed practical model of an improved organizational and management mechanism for the units of the National Guard of Ukraine is based on the principles of adaptability, multidomain, digitalization, and synergy of the security and defense sector structures. The model covers five integrated subsystems – tactical, managerial, technological, personnel, and interagency – which ensure a comprehensive increase in combat effectiveness.

The architecture of the organizational and management mechanism model for the units of the

National Guard of Ukraine is based on a multi-component approach. The NGU units are viewed as an adaptive tactical system, where each component interacts with others in real time. The model is based on the structures listed below.

1. Recon module (reconnaissance):
– various types of UAVs;
– reconnaissance teams;
– sensor networks, radio reconnaissance, thermal imaging systems.
2. Strike module (firepower):
– assault units;
– mobile fire teams;
– FPV units;
– mortar and anti-tank missile systems.
3. Support module:
– medical evacuation;
– engineering and sapper groups;
– logistics groups;
– repair units.
4. C2 platform (command and control):
– digital maps;
– automated control systems;
– tactical commander terminals;
– backup communication channels.
5. Analytical Center (reconnaissance data + modeling):
– sensor data processing;
– AI situation analysis;
– forecasting possible scenarios.

An algorithm for the rapid response of NGU units is proposed. The algorithm consists of six stages that operate in a cycle of "reconnaissance → decision → action".

1. Data collection: sensors, UAVs, and reconnaissance groups form a consolidated information package.
2. Data processing: an analytical module identifies threats, prioritizes targets, and predicts enemy actions.
3. Information transfer: the commander receives an updated battle map via a secure digital network.
4. Decision-making: the commander uses SOPs, battle cards, and calculation modules.
5. Application of forces: the modular Recon–Strike–Support group carries out the task.
6. After Action Review: the practical implementation of the operation is entered into the knowledge base, improving future actions.

The effectiveness of the model is assessed using the key indicators listed in Table 1.

Table 1 – Key performance indicators of the model

No.	Indicator	Unit of measurement	Expected result, %
1	Response time	Minutes	Reduction by 40–60
2	C2 stability during electronic warfare	Percentage of channels preserved	+35–40
3	Target detection accuracy	Percentage	+25–30
4	Effectiveness of interaction between groups	Synchronization coefficient	+30
5	Load on the commander	Number of simultaneous tasks	–20–30
6	Personnel losses	Percentage per operation	–15–20
7	Rotation and recovery speed	Days	Reduction by 10–20

The model of horizontal interaction between units provides:
– direct data exchange between Recon–Strike groups;
– minimal dependence on headquarters;
– increased C2 resilience in case of command post loss.

The model of horizontal interaction between units is implemented using autonomous tactical servers, decentralized digital maps, and shared encrypted communication channels.

The model's operating diagram is shown in Figure 1.

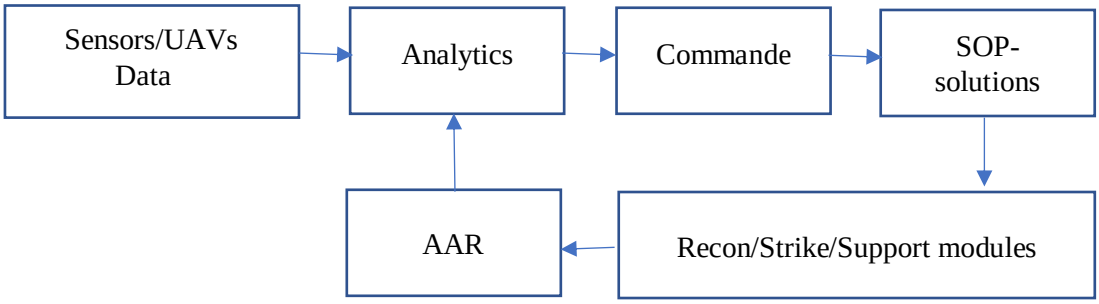

Figure 1 – Diagram of the organizational and management mechanism model for units of the National Guard of Ukraine

The cycle "Sensors/UAV → Analytics → Commander → SOP decisions → Recon/Strike/Support modules → AAR" operates continuously, which makes it possible to maintain the pace of operations and reduce the risk of unexpected losses.

Conclusion

The article substantiates the need to modernize the organizational and management mechanisms of the National Guard of Ukraine in the context of modern military-hybrid threats. A set of measures is proposed, including optimization of the organizational and staffing structure, digitization of the management system, reform of personnel processes, introduction of new technologies, and development of interagency cooperation.

The implementation of these mechanisms will increase the effectiveness of the NGU's combat and stabilization operations, strengthen national security, and ensure the readiness of forces for multi-domain operations.

A direction for further research could be the creation of a model for collecting and processing intelligence data.

References

1. Department of the Army (2022). *FM 3-0: Operations*. Washington, DC : U.S. Army [in English].

2. Joint Chiefs of Staff (2020). *Joint All-Domain Operations (JADO)*. Washington, DC [in English].

3. Kaldor, M. (2021). *New and Old Wars: Organized Violence in a Global Era* (4th ed.). Stanford University Press [in English].

4. NATO (2023). *Countering Hybrid Threats: Doctrine and Guidelines*. Brussels [in English].

5. Drobakha H. A., Oleshchenko O. A., Iokhov O. Yu., Lisitsyn V. E. (2016). *Osnovy informatyzatsii Natsionalnoi hvardii Ukrainy* [Basics of informatization of the National Guard of Ukraine]. Kharkiv : NA NGU [in Ukrainian].

6. Sporyshev K. O. (2024). *Zasady avtomatyzatsii informatsiinykh system upravlinskoho pryznachennia syl bezpeky peredovykh krain YeS ta NATO* [Principles of automation of management-oriented information systems of security forces in advanced EU and NATO countries]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, vol. 2. Retrieved from: https://surl.li/pacbbi (accessed 20 September 2025) [in Ukrainian].

The article was submitted to the editorial office 05.10.2025

УДК 351.862:355.45

Є. В. Брюхно, В. М. Синицький

ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЙ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ У ЗАБЕЗПЕЧЕННІ ДЕРЖАВНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ВОЄННО-ГІБРИДНИХ ЗАГРОЗ

Розглянуто комплекс організаційно-управлінських механізмів, спрямованих на підвищення ефективності дій підрозділів Національної гвардії України у забезпеченні державної безпеки в умовах сучасних воєнно-гібридних загроз. Акцентовано на аналізі специфіки функціонування НГУ як складової сектору безпеки й оборони, що здатна одночасно виконувати бойові, стабілізаційні, охоронні та контрдиверсійні завдання. Визначено ключові чинники, які впливають на боєздатність підрозділів: централізація системи управління, недостатній рівень цифровізації, брак висококваліфікованих фахівців, фрагментарність інформаційної взаємодії із суміжними структурами сектору безпеки. Обґрунтовано необхідність переходу до модульної побудови підрозділів за функціональними напрямами Recon–Strike–Support, що забезпечує підвищену маневреність, автономність, оперативність прийняття рішень та ефективність застосування сил у багатодоменному середовищі.

Розкрито перспективи інтеграції систем автоматизованого управління, тактичних цифрових карт, резервних каналів зв'язку й алгоритмів швидкого реагування, що дають змогу скоротити цикл «виявлення – рішення – дія» та підвищити стійкість С2 до впливу РЕБ і кібератак. Значну увагу приділено вдосконаленню кадрової політики, включно з упровадженням прискорених навчальних програм для операторів БпЛА, фахівців РЕБ, аналітиків і тактичних медиків, формуванням системи передачі бойового досвіду (AAR) та створенням єдиної бази тактичних знань. Додатково обґрунтовано модель підтримання психофізіологічної стійкості особового складу, яка передбачає застосування реабілітаційних заходів, оптимізацію ротацій та психологічного супроводу у режимі безперервної бойової готовності.

Окрему увагу зосереджено на поглибленні міжвідомчої координації через створення об'єднаних оперативних центрів, уніфікацію процедур реагування, обмін оперативними даними у реальному часі та запровадження спільних тренувальних програм зі Збройними Силами України, Службою безпеки України та іншими компонентами сил оборони. Показано, що впровадження запропонованих механізмів забезпечує суттєве підвищення оперативної стійкості, гнучкості, адаптивності та результативності діяльності НГУ, сприяючи формуванню сучасної, технологічно оснащеної та ефективної системи захисту державної безпеки.

Ключові слова: *державна безпека, Національна гвардія України, організаційно-управлінські механізми, бойові дії, гібридні загрози, організаційно-штатна структура.*

Briukhno Yevhenii – Senior Lecturer, Department of State Security, Educational and Scientific Institute of State Security, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0007-1498-8864

Synytskyi Volodymyr – Lecturer, Department of Tactical Training, Educational and Scientific Institute of Professional Education, National Academy of the National Guard of Ukraine
https://orcid.org/0009-0006-4777-8006