The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.06

A conceptual approach to improving the information support of the prospective Armed Forces of Ukraine

Oleksandr Peredrii
Candidate of Military Sciences, Senior Researcher
Head of the Research Department of the Center for Military and Strategic Studies
of the National Defense University of Ukraine,
03049, 28 Povitroflotskyi prospect, Kyiv, Ukraine,
ORCID: 0000-0003-2877-4959

Petro Snitsarenko
Doctor of Technical Sciences, Senior Researcher,
Leading Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
03049, 28 Povitroflotskyi Prospect, Kyiv, Ukraine,
ORCID: 0000-0002-6525-7064

Yurii Sarychev
Candidate of Technical Sciences, Senior Researcher,
Leading Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
28 Povitroflotskyi Prospect, 03049, Kyiv, Ukraine,
ORCID: 0000-0003-1380-4959

Viktor Zubkov
Senior Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
28 Povitroflotskyi Prospect, 03049, Kyiv, Ukraine,
ORCID: 0009-0008-5755-2339

Abstract. The relevance of this article is due to the fact that modern armed conflicts lead to a change in the nature of military operations, which increasingly acquire an informational and technological nature, which forces the leadership of the leading countries of the world to review the theory and practice of the military construction in order to implement the concept of "network-centric war". This approach involves considering the control bodies, units, planes, ships, communications, and intelligence of the armed forces as objects connected to a single information and communication network. The capabilities of such a network-centric system of conducting military operations are determined by the capabilities of the entire group of objects connected to the network (synergistic effect). In the implementation of this concept, a key role belongs to the information support of objects of a single network, which has a number of components that need to be implemented in a network-centric system of conducting military operations. The requirement for high operational efficiency of information support necessitates the widespread introduction of automated control systems (ACS) in such a system. At the same time, the information support of the objects of the unified network is the main purpose of the ACS, the means of which in automatic mode allow you to quickly display the situation, assess the terrain, the state of the enemy, your troops (forces), model the development of combat operations, develop options for solutions, draft combat documents, prove tasks to

subordinates, control their execution.

The article analyzes the experience of implementing information systems for managing the armed forces of leading countries, the peculiarities of their organization and implementation in the armies of NATO member states. Based on the results of this analysis, approaches to determining ways to improve the information support of the control systems of the Armed Forces of Ukraine are proposed. One of the main tasks of the Armed Forces of Ukraine (Defence Forces) on the way to NATO membership is the creation of a network-centric military control system, which should be equipped with ACS and compatible with the Alliance's military control systems. Meanwhile, according to foreign publications, the level of automation of the control systems of the defense forces of Ukraine today is 2-2.5% compared to the armed forces of the leading countries in the world, in which ACS ensure the level of automation of C4ISR management functions (command, control, communication, informatization, intelligence, etc.). For this reason, at present, the state of information support for the management processes of the Armed Forces of Ukraine (Defense Forces) cannot be called satisfactory. Therefore, the implementation of C-shaped ACS (taking into account the experience of the Russian-Ukrainian war) is a necessary condition for the implementation of reliable and sufficient for the implementation of network-centric principles of conducting operations (combat operations) in the prospective structure of the Armed Forces of Ukraine.

Thus, the realization of such a conceptual approach to the implementation of information support (by its main types) in the C-shaped ACS will contribute to increasing the combat capabilities of the troops (forces) of the Armed Forces of Ukraine (Defense Forces) in the modern conditions of conducting military operations.

The materials of the article can be useful for the higher command staff of the Armed Forces of Ukraine (Defence Forces), as well as scientists and researchers in the field of information support and development of the defense sphere of the state.

Keywords: Information Systems; Control Systems; ACS, Network-Centric Warfare.

Introduction

The analysis of the publications shows that today the issue of forming the future outline of the Armed Forces of Ukraine (AF of Ukraine) is being actively researched, taking into account the experience of the leading countries of the world. The content of the concepts of the construction and development of the armed forces of the countries of the world convincingly shows that the priority areas include the improvement of the military (force) control system (Ilyashov, 2009), (Pashchetnyk, 2015), (Zagorka, Koval, Tyurin, Malyuga, Zagorka, 2016). At the same time, the experience of the participation of the armed forces of the leading countries in the operations of the late 20th and early 21st centuries determined the development and implementation of the concept of *Net-Centric Warfare* (*NCW*) as the main trend in the development of the theory and practice of military management (Savin, 2011), (Kondratiev, 2009), (Baulin, Kondratiev, 2009), (Makarenko, Ivanov, 2018), (Oproschenko, 2018), (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Nor, Borokhvostov, Solomytskyi, 2023). These publications claim that a network-centric war is a war in which the achievement of success is ensured on the basis of information superiority over the enemy by means of combining military objects into a single information network (US military doctrine, 2020), (Gavrilov, 2010), (Balakhontsev, Kondratyev, 2011).

The above publications mainly explore the fundamental tasks of building automated control systems (ACS) for the implementation of the concept of network-centric wars. At the same time, they do not pay enough attention to the information support of such systems. Without up-to-date information, any automated system cannot perform its intended functional tasks. At the same time, the information advantage can be achieved by timely information support of the decision-making

process and actions at all levels of the military (force) control system. Therefore, the issue of information support of modern control systems in the military sphere is of the utmost importance.

The purpose of the article is to justify conceptual approaches to determining the directions (ways) of improving the information support of the control system of the Armed Forces of Ukraine based on the experience of building and using information systems for managing the armed forces of the leading countries of the world. In this article, only the main contours of the development of control systems in the conditions of fundamentally new wars of the 21st century are marked.

Presenting the main material. The war of the future is not only a high-tech war, but primarily a "network" war. It requires the unification of all participants in the hostilities, the support of accurate and timely data on the situation on the battlefield in real time to ensure preemptive damage to enemy objects (Makarenko, Ivanov, 2018), (Oproschenko, 2018), (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020).

The reform of the armed forces of the leading countries of the world is carried out, first of all, by introducing new approaches to the management and conduct of hostilities. They are based on the network principle of providing troops (forces) with accurate and timely information, provided by the promising "network-centric" concept (Gatsenko, 2015).

Today, the concept of information has many definitions. For the military sphere, it is reasonable to consider that in general, *information* is processed and understood data, their content, meaning (essence), knowledge or conclusions obtained on their basis, regardless of the form of presentation (Central Department of Metrology and Standardization of the Armed Forces of Ukraine, 2014). At the same time, the value of information is determined by its usefulness and its ability to provide a certain subject with the necessary conditions to achieve the goal.

It should be noted that according to the laws of cybernetics (Wiener, 1968), any control function in systems is implemented exclusively through information. This means that the process of any management, and especially in the military sphere, requires the implementation of a number of information processes that have an impact on all elements of the control mechanism. The set of these information processes is actually united by the information support definition, which permeates the closed loop of management. Its essence consists, on the one hand, in the formation of tasks and their delivery from the control body to the subjects of the system, and on the other hand, in the possibility of the control body receiving feedback to control the management process and adjust the information impact. The above is summarized by the following relevant definitions given in the Military Standard (Central Department of Metrology and Standardization of the Armed Forces of Ukraine, 2014).

Information support (in the military sphere) is a set of measures of military administration bodies of all levels, actions of troops (forces) and other subjects of information activity with the aim of creating (forming) and using in the information space of the military sphere the necessary information resources for the implementation of management processes in the state defense interests.

The information space of the military sphere is a part of the information space of the state: an environment in which information processes and information relations regarding the creation, collection, receipt, storage, use, distribution, security and protection of information (information products, information resources) of a military nature take place.

Integral components of the information environment are information resources, information infrastructure and information technologies, which constitute the essence of the national information potential.

An information resource is data and knowledge, the distinguishing and integral characteristic of which is their pragmatic value, which is determined by practical needs in the interests of solving certain tasks.

Information infrastructure is a set of various information (automated) systems, information resources, telecommunication networks and data transmission channels, means of communication

and control of information flows, as well as organizational and technical structures, mechanisms that ensure their functioning.

Today, it is the level of information potential which is based on the information resource produced by the elements of the information infrastructure, and the possibility of its effective, in particular automated, use, that to a greater extent determines the high efficiency and quality of decision-making. In addition, it also determines the necessary structure and characteristics of control bodies, weapons samples, assessment of their sufficiency level, in general – with a high probability determines the outcome of an armed confrontation.

On the basis of scientific research (Sarychev, 2016), a complete list of information functions, which implement the components of information support of the control system in the military sphere, was formed. Such components should at least include the following main types:

Condition monitoring is a set of activities that implements a continuous process of obtaining information of a military nature based on data of all types of military intelligence, with the aim of assessing and forecasting the development of the operational and tactical situation, as well as highlighting threatening actions in space, air, land, surface, underwater and information spaces.

Information-analytical support is a set of activities that implements the processes of creating information products based on the use of information resources, conducting calculations, modeling situations, analyzing data and information in order to support decision-making by military control bodies.

Organization-administrative support is a set of organizational and administrative measures that are implemented by military control bodies, commanders (supervisors) through document circulation for the purpose of preparing and making informed decisions, communicating tasks to subordinates, organizing execution and control.

Protection of information resources is a set of legal, administrative, organizational, technical and other measures that ensure the preservation and integrity of information (information resources) and the proper order of access to it (them).

Moral-psychological support is a set of measures that are carried out with the aim of forming, maintaining and renewing the moral-combat and psychological qualities, moral-psychological state of troops (forces) in the personnel of military formations at the level necessary for the successful performance of assigned tasks.

Image support is a set of activities carried out to highlight the activities of the Defense Forces, with the aim of forming a positive public opinion in society and at the international level, as well as promoting the growth of the prestige of the military service in the national society and beyond.

Disinformation support is a set of measures to mislead the enemy by means of distracting demonstrative actions, imitation, concealment of one's main actions and dissemination of false information.

Information-psychological influence is a purposeful informational intervention in the consciousness (subconsciousness) of the leadership and personnel of the enemy's troops with the aim of introducing changes in behavior and (or) worldview that undermine their moral-psychological state.

Information-technical impact is a set of actions and attacks that implement purposeful destructive electronic interference in the process of functioning of the enemy's information infrastructure objects.

Radio-electronic protection is a set of measures to guarantee the stability of the operation of radio-electronic components of information means, information systems and other media of information resources in conditions of radio countermeasures by the enemy and mutual electromagnetic influence.

Navigational support is a set of measures aimed at constant and objective acquisition of information by military facilities about their own location in real time for the effective conduct of operations (combat operations) and the use of weapons and military equipment.

Topo-geodetic (geo-informational) support is a set of measures for the preparation and delivery of all levels of topographic and special maps (including electronic ones), photo documents of the area,

as well as astronomical-geodetic and gravimetric data to the military control bodies for the implementation of spatial synchronization in the control of troops (forces) and weapons in the course of performing the tasks set by them.

Hydrometeorological support is a set of measures to collect, analyze and deliver information about the hydrological and meteorological situation to the troops (forces).

The specified types constitute the basic list of components of the complete process of information support of the control system in the military sphere, which implements management functions according to the target purpose.

In the modern era of the "information age" (Digital Age, Computer Age), new information technologies come to the fore. Their implementation in the military sphere is also aimed at increasing the combat capabilities of formations. However, not only due to the improvement of intelligence, fire, maneuverability and other characteristics of individual samples (platforms), but, first of all, due to the availability of better information support and the possibility of shortening the cycle of combat control in operations (battle) (Kondratyev, 2008).

The concept of "network-centric war", or "conducting hostilities in a single information and communication space", considers elements of the armed forces as devices connected to the network. Depending on the choice of network architecture and its type, the means of the network can be military units and subdivisions, ships, aircraft, weapons, control, communications, intelligence, and a combination of both. The capabilities of such combat units are determined not so much by individual characteristics, but by the capabilities of the entire group of networked assets as a whole.

According to specialists' calculations, the automation of the processes of collection, processing, generalization, transmission (reception), use of information can contribute to increasing the combat capabilities of troops (forces) by 15-20% and, at the same time, reduce the time spent by military control bodies of all levels by 50% on making decisions and bringing tasks to subordinates (Frolov, 2012).

Ensuring comprehensive integration, increasing the level of interaction due to the implementation of the principles of new network-centric concepts and the integration of control, communication, intelligence and defeat systems is becoming an increasingly urgent and priority direction of reforming the armed forces of most countries of the world.

Measures for the implementation of network-centric concepts are mainly carried out in three key areas (Snitsarenko, Sarychev, Tkachenko, Zubkov, 2021):

development of information acquisition, processing, analysis and distribution systems using unified tools for its processing and transmission formats;

optimization of organizational structures of control bodies, information processing and analysis, personnel training and review of doctrinal documents;

deployment of modern communication and data transmission systems.

It is known that NATO implements the concept of "Complex network capabilities" (NATO *Network Enabled Capabilities - NNEC*), which is intended to organize the interaction of high-tech formations of national armed forces in armed conflicts (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Molitvin, 2008), (Adams, Ben-Ari, Logsdon, Williamson, 2004). Its implementation will enable effective information support of operations of the entire possible spectrum, starting from peacekeeping operations to establish peace to large-scale combat operations of high intensity. At the same time, NATO military experts emphasize that NNEC is not only the integration of control and communication systems, but also an opportunity to increase the level of information interaction of all participants in the operation (combat operations), including weapons, bodies and logistical points software.

In the USA, the essence of the concept of "network-centric war", "conducting hostilities in a single information and communication space", based on the experience of using troops (forces) in modern conflicts, has acquired the greatest practical content in the unified system of intelligence and

information support and combat control of the US Armed Forces - "*Network Centric Warfare*" (*NCW*) (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Molitvin, 2008), (Adams, Ben-Ari, Logsdon, Williamson, 2004), (Thomas, 2005).

Great Britain (*Network Enabled Capability*), France (*Guerre Infocentre*), Germany (*Infanterist der Zukunft*) and together with the Netherlands ("*Tactical Edge Networking*") (Adams, Ben-Ari, Logsdon, Williamson, 2004), Australia (*Network Centric Warfare*) (Adams, Ben-Ari, Logsdon, Williamson, 2004), China have similar systems (*Integrated Network-Electronic Warfare - INEW*) (Thomas, 2005), and Israel considers the implementation of information technologies as an integral and mandatory attribute of modern and future operations (Adams, Ben-Ari, Logsdon, Williamson, 2004).

It is obvious that the main principles of the implementation of measures for the wide introduction of information components in the military sphere within the framework of the network-centric operations concept are:

ensuring real information unity of groups;

application of open architecture and modular construction of modern systems and complexes of armed struggle;

implementation of vertical and horizontal information integration and interaction of all participants of the operation (combat operations).

Analysts claim (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020) that the wars of the next generation are, above all, wars of intelligence, where having the necessary information about the enemy is the key to success in such wars. In modern conditions, in the leading countries of the world, a steady trend can be seen to emphasize the acquisition and integration of various information about the state of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational, and other relations between states, groups of states and in the world as a whole.

Therefore, such a type of information support as enemy monitoring, which is based on the process of comprehensive intelligence, is dominant in the general information support system of troops (forces). At the same time, any network-centric system cannot be used as intended without up-to-date information in real time. Depending on the level, the network-centric system, based on the presence of useful, reliable, complete, timely intelligence information, is able to visually display the situation, assess the terrain, the state of the enemy and its troops (forces), and simulate the development of combat operations. At the same time, the system is able to produce recommendations, options for solutions, drafts of combat documents, deliver tasks to subordinate control points and the ability to control all information processes.

Reliability is the ability of information to reflect real objects (processes, phenomena) with the required accuracy within a certain level of probability of the case being displayed.

Sufficiency (completeness) is the minimal, but sufficient composition of the information product for making a decision.

Timeliness of information means that it is exactly what is needed at the moment, essential, important at this time.

The need (usefulness) of information is determined in view of the tasks that can be solved with its help.

Along with the advantages of the network-centric concept of conducting hostilities, a number of problems regarding its implementation have been identified. In particular, the issue of rational distribution and processing of large volumes of information received by consumers is acute. For a better understanding of this problem, we consider it expedient to dwell on the distribution of classes of network-centric systems depending on the degree of automation of controlled processes and information flows that circulate in them.

The experience of development, implementation and operation of network-centric systems in

the USA shows (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (American ACS) that modern automated control systems, which are informational in nature, are divided into several classes. According to the functions performed by the systems, command, control, communications, computers (informatization), general intelligence, surveillance, real-time intelligence (*Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*) are distinguished.

At the same time, the systems differ in the degree of automation of controlled processes in accordance with this classification. Each system belongs to a specific class according to the level of automation of management functions. So, if the control system in the automated mode has only two functions, for example, command and control (*Command and Control*), then it will correspond to the "CC" class (C2). If four functions are automated in the system - command, control, communication, communication (*Command, Control, Communications, Computers*), then such a system is classified as "CCCC" (C4). At the same time, functions starting with the letter "C" are used as basic, and others are additional.

From the point of view of automated management functions (tasks), the control system, which contains more letters "C" in its abbreviation, is more perfect. Thus, the C2SR (*Command, Control, Surveillance, Reconnaissance*) class system will be inferior to the C4 class system in terms of the range of tasks used in automated mode.

Systems in which *Command and Control* (C2) functions are automated solve the following tasks:

display and transmission of combat tasks to subordinate control bodies (control objects) in a formalized text and graphic format using a single network;

determination of the positions of own control objects and notification of their control bodies and neighbors about their location with display on electronic maps;

display on electronic maps and data exchange about detected enemy objects, infrastructure elements on the battlefield;

selection and calculation of traffic routes based on known data about the road network and display of the route traveled.

The C2 system only allows the commander to quickly convey the decision to subordinates and control the progress of its implementation. At the same time, the function of assessing the situation and making a decision is fully dependent on the person. Some systems belonging to the C2 class can perform mutual recognition of objects located in the system according to the principle of "friends-or-foes". In addition, they can also perform target identification and provide automatic target designations to the means of fire damage included in the system. Control systems in which such functions are automated have additional letters "SR" (*Surveillance, Reconnaissance*) and are designated as C2SR (or C2+). At the same time, computers used in C2 class systems are considered only as means of primary processing and display of information. Although C2 systems include personal computers, they do not have the word "*Computers*" and the corresponding letter in the abbreviation of their class. In general, the C2-class system only helps commanders communicate the task to subordinates, collect and display current information about the enemy and the state of their control objects. At the same time, there is still no talk of intellectual support for decision-making and the development of options for combat decisions and their simulation.

Such tasks as the automatic organization of communication and local computer networks are already a distinction of the system, which has the abbreviation of the word *Communications* (C3) in the name of its class. The tactical link systems in service with foreign countries belong to the C2 or C2+ class and differ from each other only by a small expansion of the spectrum of the solved tasks. At the same time, all systems of tactical purpose do not even reach the C3 class in principle.

The presence of the fourth letter "C" (*Computers*) and the letter "I" (*Intelligence*) in the abbreviation of the system class means, firstly, full automatic processing of the data obtained during the implementation of the first two "C" - *Command and Control*, secondly, on the basis of the primary

data processing the development of a variant of the commander's situational decision and its presentation in the most convenient form for a person, respectively.

C4 class systems (in addition to performing the functions implemented in C2 and C3 class systems) must be able to solve the following tasks:

full automation of information collection and processing;

informational support for the development of decision options by the commander (availability of "Sketch in the decision" type programs - the intention of the decision);

simulation of combat operations based on selected options for performing combat tasks with a graphic display of their progress and results on electronic maps, including using means of a three-dimensional display of the battlefield;

informational support for the development of planning documents ("Sketch in the plan" program, which transforms graphic and audio materials into planning documents;

informational support for decision-making during a combat mission (updating assessments and conclusions based on information received during combat).

The fundamental difference between the C4I class systems and the C2 class is a higher degree of automation of information and control tasks.

In the armed forces of even technologically developed countries, C4I and C4SR class systems belong to the operational or operational-strategic link systems according to the level of control. According to military experts (Adams, Ben-Ari, Logsdon, Williamson, 2004), the main obstacles to the development of tactical link systems from class C2 to class C3 and C4 are:

the absence of mathematically correct algorithms for evaluating the actions of the troops at the tactical level, taking into account the huge variety of methods and techniques used by them to perform combat tasks;

the difficulty of creating an automated system for collecting and evaluating data on the tactical situation, given the wide variety of its parameters and the rapidity of changes (compared to the operational control chain);

the need to process a large amount of data per unit of time, the volume of which currently exceeds the capabilities of the machine support used in the tactical control chain;

the difficulty of creating communication networks and reliable local networks (data transmission systems) between a large number of highly mobile control objects.

At present, significant development of C+ class systems in the interests of implementing the concept of network-centric operations has been received in the USA.

The most famous of all the existing systems of the tactical link is the American system of the "C2SR" class FBCB2 - Force XXI Battle Command Brigade and Below ("*System of managing the brigade and subordinate units in the battle (battle) of the twenty-first century*") - one of the main components of the automated control system US ground forces ABCS (*Army Battle Command System*), which played a key role in the operations in Iraq and Afghanistan (Thomas, 2005).

During the last 30 years, the military-political leadership of Ukraine, realizing the need for the development of military control systems, paid attention to the process of creating automated military control systems of various levels. Thus, in order to solve the problems of the management of the Armed Forces of Ukraine as a whole, the concept of the functioning and development of such systems was developed, starting with the Unified Automated Control System of the Armed Forces of Ukraine (UAMS of the Armed Forces of Ukraine), which was supposed to be integrated with other state ACS. Within the framework of the creation of the UAMS of the Armed Forces of Ukraine, the development of special and other ACS of various levels of military control bodies (tactical, operational, operational-strategic) was foreseen: ACS of the "Dnipro", "Karpaty", "Oreanda", "Nika", "Borsuk", "Space" and others. At the same time, special emphasis was placed on the introduction of modern information technologies in the management of troops, military equipment and weapons during the creation of the UAMS of the Armed Forces of Ukraine.

During this time, more than 100 scientific research works and more than 40 research and design works were carried out on the subject of UAMS of the Armed Forces of Ukraine. The experience of carrying out such works has proven their low efficiency. Thus, only about 20% of works reached the stage of production of prototypes, experimental operation and state tests. And about 80% of them did not find their implementation, so they were suspended at various stages of work: sketch and technical design (40%), development of design documentation (40%) (Pastukhov). According to experts, the imperfection of research works was influenced by many problems of a general nature. One of the main ones is the lack of adequate experience in the development of complex, multi-branched automated systems for military purposes in the majority of Ukrainian development organizations.

Nevertheless, today the main idea of the creation of the UAMS of the Armed Forces of Ukraine – the automation of the necessary types of activities of the military control bodies – has already been implemented in general. During this time, separate components of ACS of various levels were developed (information and analytical systems for supporting the control of the organizational and personnel structure and personnel; monitoring and planning of defense resources; modeling of prospective military formations and organizational measures for the implementation of directives; creation and development of weapons and military equipment) and they actually function in a protected mode at the facilities of the Armed Forces of Ukraine.

However, it should be noted that at this stage of the development of the Armed Forces of Ukraine, the state of automation of management processes cannot be called satisfactory. According to (Gatsenko, 2015), the automation of the activities of military administration bodies is only 10-30% of the needs. The available means do not make up complete systems, the existing information and calculation resources meet the needs of control bodies by only 12-15%. At the same time, the level of informatization of the control systems of state defense entities compared to the armed forces of the leading countries of the world is 2-2.5%. At the same time, the presence of large screens with icons of different colors on the electronic topographic map at the control point is not a sign of a high level of automation of the troop control system. In addition, before the start of the armed aggression, despite a number of attempts, the construction of an automated combat control system for troops (forces, weapons) was not completed in the Armed Forces of Ukraine (Galagan, Polishko, Bondarchuk, 2019). It turned out that such a task became too difficult.

At the same time, in this context, the top military leadership of Ukraine defined a vision for the development of the military (force) control system (Mil, 2020): "... It is necessary to build a reliable system of communication, automation, intelligence and surveillance (C4ISR) in the Armed Forces of Ukraine, resistant to external influences, protected from means of electronic warfare (EW), which will have alternative communication channels. The means of communication must be combined with the means of communication of the partner countries. It is necessary to create an information network in the interests of the security and defense sector of the state, which will ensure the acquisition of information capabilities for receiving, processing, storing, transmitting, controlling and providing information at the request of commanders and headquarters (tactical, operational, strategic levels) of the United forces".

With the beginning of the armed aggression of the Russian Federation against Ukraine in 2014, the highest military and political leadership of Ukraine paid special attention to the issue of the development of the ACS by troops (forces, weapons). The result of this, already after the full-scale invasion of the armed forces of the Russian Federation into Ukraine, is the adoption by the Armed Forces of Ukraine in 2022 of the "Dzvin-AS" ACS - a highly integrated automated combat control system of troops (forces) of the strategic, operational and partially tactical level. It is believed that it enables (Mil):

to generate combat control documents in semi-automatic and automatic modes;

to receive available intelligence on the enemy's troops, their current and prospective support;

to create and monitor cartographic information;

to receive comprehensive data on own troops;

to carry out calculations of the ratio of forces and means, the optimality of their use in various scenarios.

In addition, with the start of the hostilities in 2014 in the East of Ukraine, the combat control system of the "Kropyva" ("Nettle") tactical unit was successfully operational in a short period of time. This is a battle-tested system designed to automate individual control tasks at the level of a battalion - company - platoon - a separate unit of equipment (cannon). Currently, the "Kropyva" ACS can be used by various units of the ground forces: artillery, infantry, tank units, joint military intelligence, air defense units of the Graund Forses, sapper units, etc. At the same time, a protected Delta situational awareness information system was implemented for the military control bodies of the Ukrainian Armed Forces. It allows collection, processing and display of the situation in real time, and also provides support for decision-making by the commander.

In our opinion, making an attempt to immediately create a C4ISR system is a task that does not correspond to the resource capabilities of the state. As an example, a special NCOIC consortium (96 companies from 32 countries, 26 of which are NATO members) was formed to optimize the implementation of the NATO concept *Network Enabled Capabilities* (NNEC). It is intended to ensure the unity of information processing protocols and the coordination of industry efforts in fulfilling the requirements for achieving the necessary level of interaction and integration of prospective systems in order to ensure the implementation of network-centric principles of military formation management.

At the same time, according to the conclusions of American analysts, none of the European allies is likely to be able to create a fully networked army in the near future. The biggest challenge for European investment in C4ISR is the general limitations of defense budgets, not the lack of adequate technology (Adams, Ben-Ari, Logsdon, Williamson, 2004).

In this matter, it is advisable to borrow the experience of China as well. Its military experts realize that they will not be able to create a network-centric system adequate to the American one, despite the presence of a significant military budget, in the near future. Therefore, the bet is placed on the creation of forces, systems and means that provide an asymmetric effect on the enemy. It means the fire and electronic defeat of elements of information structures (command posts, communication nodes, orbital grouping of intelligence and control satellites, etc.) (Thomas, 2005).

In view of the above, it is advisable to start the development of the C-shaped system in Ukraine from the C2+ level, with its subsequent evolutionary increase to C3 and higher, based on the results of tests, operational experience and resource capabilities. At the same time, it should be remembered that information support of control bodies is a priority task - without information, any control system works inefficiently. Only with the availability of relevant information the system can perform functional tasks as intended.

In our opinion, the level of information support of troops (forces) in the interests of reliable operational management should ensure:

for the tactical level (platoon, company, battalion, brigade) - using the C2+ type system, solving the following tasks:

exchange of information about the position, detected objects of the enemy and their actions in an automated mode in real time with display on electronic maps from top to bottom and from bottom to top;

determination of the positions of own control objects and notification of their control bodies and neighbors about their location with display on electronic maps;

transmission of combat tasks to subordinates in a formalized text and graphic format and control of their progress;

mutual recognition of objects located in the system according to the principle of "friends-or-foes";

identification of targets and providing in an automated mode targeting of means of fire damage;

for operational and strategic levels - using a system of the C3 type (in the future - C4 with applications), which must be able to solve the following tasks:

full automation of the collection and processing of information in a real (close to real) time scale about the enemy, the position and condition of own troops (forces);

informational support for the development of decision options for the use of the Armed Forces, troops (forces), formations and military units;

simulation of operations (combat operations) according to the selected options with a graphic display of their progress and results on electronic maps, including using three-dimensional display tools;

information support for the development of planning documents, conversion of graphic and audio materials into planning documents;

informational support for clarifying decisions during operations (combat operations).

Results

Thus, the experience of the world's leading countries convincingly shows that when implementing a network-centric concept for the control systems of the Armed Forces of Ukraine, the main attention should be focused on the issues of collection, processing, analysis, identification and security of information to support decision-making by managers at all levels. At the same time, the support of timely, up-to-date, reliable (relevant) information for military assignment control systems becomes the main task in the general process of information support of the Armed Forces of Ukraine.

The conducted analysis shows that the activities related to the construction and use of information systems for the control of the armed forces of the leading countries of the world, first of all, the experience of the NATO member states, causes an urgent need to further search for approaches to the improvement of the information support of the control systems of Ukrainian Armed Forces. The network war can be won only by network means, adapting to one's own conditions and effective technologies.

Conclusion

1. The concept of network-centric wars is a system of views on the conduct of hostilities and military-technical support in the conditions of full computerization of forces and means of armed struggle. At the same time, the interoperability of automated intelligence systems, control of troops and weapons, as well as ensuring sustainable interaction between them are considered as key components. They are necessary to achieve an informational advantage and, as a result, an advantage in decision-making in order to decisively anticipate the enemy throughout the entire cycle of combat control (according to the principle: "the first to see - the first to shoot").

2. Information support of network structures becomes the main and necessary condition for the effective functioning of control systems. In order to create such a structure and a single information space for users in a real (close to real) time scale, it is necessary to combine all forces and means of obtaining and generating information by automated systems.

3. Proper and timely information support of military control systems is a necessary condition for the implementation of network-centric principles of combat operations. It can be implemented in the Armed Forces of Ukraine by introducing a C-shaped automated control system through its evolutionary development, starting with the construction of a C2+ class system. In this case, taking into account the great experience gained by the US armed forces in the development of informatization of the military sphere, the implementation of the theory of network-centric operations into practice, as well as the fact that Ukraine is in a state of war, we consider it appropriate:

to take as an example for implementation in the Armed Forces of Ukraine the existing American automated control system of the tactical link of the C2SR class - Force XXI Battle Command Brigade and Below (FBCB2) or another similar prospective automated control system of foreign production;

at the first stage, as an urgent measure, consider the issue of obtaining (purchasing) a brigade set of an automated tactical link control system for testing in the conditions of conducting real combat operations to determine the feasibility of further implementation in the Ukrainian Armed Forces;

in the case of obtaining positive results, raise the issue of gradually equipping military units and units of the Ground Forces of the Ukrainian Armed Forces with prospective automated tactical control systems of foreign production;

at the same time, to direct the acquired experience to the development of domestic (taking into account the capabilities of science and industry of Ukraine) C-shaped prospective adaptive control systems of various levels, compatible with the automated control systems of the armed forces of NATO member countries.

Recommendations

It is advisable to direct further research to the development of information support of the Ukrainian Armed Forces by more clearly defining the composition, structure and volume of information flows. They circulate in control systems, substantiating the functional components of the information process in such systems, which will allow optimizing the list of tasks that must be performed at each stage of the control cycle.

The materials of the article can be useful for the higher command staff of the Ukrainian Armed Forces (Defence Forces), as well as scientists and researchers in the field of information support and development of the defense sphere of the state.

References

1. Ilyashov, O. A. Trends in the development of armed struggle in the wars of the fourth - sixth generations. (2009). *Science and defense*. No. 3. P.43–48.
2. Pashchetnyk, O. D. Analysis of global trends in the development of automated systems for the management of troops and weapons. (2015). *Science and technology of the Air Force of the Armed Forces of Ukraine*. No. 2 (19). P.64–68.
3. Peculiarities and principles of building a network-centric management system of a group of troops (forces). (2016). O.M. Zagorka, V.V. Koval, V.V. Tyurin, V.G. Malyuga, I.O. Zagorka. *Collection of Scientific Papers of Kharkiv Air Force University*. Issue 3(48). P. 7–11.
4. Savin, L. V. Network-centric and network warfare. Introduction to the concept. (2011). Moskov: Eurasian Movement. 130 p. Access mode: https://www.geopolitica.ru/sites/default/files/ ncw.pdf.
5. Kondratiev, A. Implementation of the concept of "Network-centric warfare" in the US Air Force. (2009). *Foreign Military Review*. No. 5. P.44–49. Access mode: http://pentagonus.ru/publ/ 24-1-0-1159.
6. Baulin, V., Kondratiev, A. Implementation of the concept of "Network-centric warfare" in the US Navy. (2009). *Foreign Military Review*. No. 6. P. 61-67. Access mode: http://pentagonus.ru/publ/26-1-0-811.
7. Makarenko, S. I., Ivanov, M. S. *Network-centric warfare – principles, technologies, examples and prospects*. (2018). SPb: High technology, 898 p.
8. Oproschenko, Yu. O. Network-centric war: main features, peculiarities and principles of conduct. (2018). *Social and political studies*. Scientific almanac. Works of young scientists. No. 2. P. 7-11.
9. Theoretical foundations of managing a group of troops (forces) in modern conditions of armed struggle (2020). Monograph. Zagorka, O. M., Pavlikovsky, A. K., Koretskyi, A. A., Kyrychenko, S. O., Zagorka, I. O. In general ed. Russian, I. S. Kyiv: NUOU named after Ivan Chernyakhovsky. 248 p.
10. Nor, P. I., Borokhvostov I. V., Solomytskyi O. I. The main trends in the development of forms and methods of armed struggle. *Science and defense*. 2023. No. 1. P. 20-27.
11. US military doctrine "Joint Vision 2020". (2020). Access mode: http://pentagonus.ru/doc/ JV2020.pdf.

12. Gavrilov, A. Automated system for collecting, processing and distributing intelligence information of the US Army DCGS-A. (2010). *Foreign Military Review*. No. 7. P.32–40. Access mode: http://pentagonus.ru/publ/122-1-0-1596.
13. Balakhontsev, Y., Kondratyev, A. The influence of the "network-centric war" concept on the effectiveness of intelligence support for the US Armed Forces. (2011). *Foreign Military Review*. No. 2. P.14–20.
14. Gatsenko, S. S. Analysis could be used for military management systems and their improvements. (2015). *Collection of scientific works of the CVSD NUOU*. No. 2. P. 85–90.
15. Military standard VST 01.004.004 – 2014 (01) "Information security of the state in the military sphere. Terms and meaning" (2014). [confirmed by the order of the head of the Central Department of Metrology and Standardization of the Armed Forces of Ukraine - the chief metrologist of the Armed Forces of Ukraine dated 02/27/2014. No. 1].
16. Wiener, N. *Cybernetics or control and communication in animals and machines*. (1968). Moskov. Soviet Radio. 328 p.
17. Sarychev, Yu. O. Analysis of approaches to determining the modern role and place of information support in the state administration system. (2016). *Bulletin of the NADU under the President of Ukraine*. In general ed. Kovbasyuk, Yu. V. Issue 3 (82). P. 138–143.
18. Sarychev, Yu. O. Theoretical approach to information support in the system of state administration in the military sphere. (2016). *Bulletin of the NADU under the President of Ukraine* (Series "State Administration"). In general ed. Sausage, Yu. V. Issue 4 (83). P.153–160.
19. Kondratyev, A. E. General characteristics of network architectures used in the implementation of promising network-centric concepts of leading foreign countries. (2008). *Military Thought*. No. 12. P. 63–73.
20. Frolov, V. S. Structural and logical scheme of the Unified automated control system of the Armed Forces of Ukraine. (2012). *Science and defense*. No. 1. P. 15.
21. Snitsarenko, P. M., Sarychev, Yu. O., Tkachenko, V. A., Zubkov, V. P. The experience of the armed forces of the leading countries of the world in the interests of improving the information support of the Armed Forces of Ukraine. (2021). *Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi*. No. 2 (72). P.40-50.
22. Molitvin, A. On the implementation of the concept of a single NATO information space. (2008). *Foreign Military Review*. No. 1. P. 23–27. http://pentagonus.ru/publ/3-1-0-565.
23. Adams, G., Ben-Ari, G., Logsdon, J., Williamson, R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
24. Thomas, T. L. (2005). Chinese and American network warfare. *Joint Force Quarterly*. July.
25. American ACS troops FBCB2. Access mode: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com.
26. Pastukhov, A. ACS of the Armed Forces of Ukraine. Technologies. Access mode: https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/#google_vignette.
27. Galagan, V. I., Polishko, S. V., Bondarchuk, S. V. Proposals for improving the process of introducing information systems of foreign production into the activities of the Armed Forces of Ukraine. (2019). *Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi*. No. 2. P. 62–68.
28. The Vision of the General Staff of the Armed Forces of Ukraine regarding the development of the Armed Forces of Ukraine for the next 10 years. (2020). https://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi – 10 - rokiv.
29. The "Dzvin-AS" management system has been adopted by Ukraine. Access mode: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny.