Information systems research

UDC 621.391 **doi: 10.20998/2522-9052.2018.2.08**

D. Kisel [1], O. Salnikova [2], S. Antonenko [2], A. Shyshatskyi [3]

[1] Military unit A 0135, Kyiv, Ukraine
[2] National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine
[3] Central research Institute of weapons and military equipment of Armed Forces of Ukraine, Kyiv, Ukraine

ANALYSIS OF INFORMATIONAL COUNTERACTION INFLUENCE ON ORGANIZATION OF OFFICERS MANAGEMENT ACTIVITY

Due to the increase in active use of modern information technologies as one of the means of armed struggle the strategy and tactics of conducting modern wars and military conflicts has changed. To this end, the authors of this article considered the concept of information countermeasures and its impact on the organization of managerial activities of officials. In the course of the study it was established that the leadership of many countries of the world developed the concepts of information wars, taking into account the information vulnerabilities of the conflicting parties, practical implementation of these concepts is carried out through information (information-psychological) operations. The analysis of the military-political leadership views of some developed states of the world on information warfare showed that it has three components: information, technical (information operations), and information-psychological (information-psychological operations). As a result of the study conducted by the authors of this article, it is proposed to adjust the regulatory documents and to take into account additional destructive factors for the organization of managerial activities of officials, namely, information countermeasures. Also, the authors of the article proposed to change the system of management training, with the purpose of training the latter to make correct and deliberate decisions in the context of information confrontation.

Keywords: information confrontation; management; decision-making; information technologies; information warfare.

Introduction

The ongoing revolution in information technology marks a new stage in the development of military systems [1-5].

There are terms "information weapons" and "information warfare" increasingly began to meet in the press, which, in effect, mean a revolution in the art of war [3-9].

After all, these terms conceal fundamentally new forms of warfare, in which the suppression of the enemy is achieved through the massive use of information weapons, considered by highly developed countries experts as the decisive factor in owning the modern world.

The use of information weapons and information and psychological impact is already in many ways capable to achieve the same results as the large-scale conventional or even nuclear war [1-11].

The most important attribute of the management process in military systems is information. At all stages of the historical development of military affairs it appears as an object of fierce fighting. Information warfare waged in almost all wars, and even the ancient generals believed that "the best war is to break the enemy's plans [12]."

From the First World War to the operation in Yugoslavia a huge historical experience of information warfare was accumulated by the US. In the early 90s the US government instructed the Ministry of Defense to summarize the existing experience of fighting against the enemy management system within the concept, called information warfare concept. It should be noted that similar concepts of information warfare adopted in the UK, Germany, France, other countries of NATO and Russia.

Information warfare is one of the main threats to national security of Ukraine in the XXI century. This is supported by an active practical implementation of the concept of information warfare and isolating for these purposes considerable financial resources of the Russian Federation.

In this state, the arsenal of information war is growing at an accelerated pace, including both special software and hardware, computer viruses, "logical bombs," and the means of psychological and parapsychological impact [13].

The report of the Joint Security Commission, established by order of the Secretary of Defense and the Director of the CIA in the United States in June 1993 and completed in February 1994, said: "... It has already been recognized that data networks are becoming the battlefield of the future. Information weapons, whose strategy and tactics of application have yet to be carefully worked out, will be used with "electronic speeds" in defense and attack. Information technology will allow resolving geopolitical crises without producing a single shot.

Our national security policy and procedures for its implementation should be aimed at protecting our capabilities to conduct information wars and to create all the necessary conditions for prohibiting the warring states of the United States to wage such wars..."

Proceeding from the foregoing, ***the purpose of this article*** is to conduct an analysis of the impact of information counteraction on the organization of managerial activities of officials.

Presentation of the main material

At present, there are ideas that mankind has overcome three "waves" in its evolution:

1) agricultural, which began 10,000 years ago;

2) commercial, which began 300 years ago;

3) technological (or information) extending at present.

The first two waves of civilization brought a revolutionary change. The information wave, as in the first two cases, determines its economy, the media, political institutions, and, of course, its own way and nature of warfare. Awareness of these processes led to the emergence of the term information war. According to US military experts, information technologies emerging as a result of the third wave are able to "revolutionize" the process of conducting operations (combat operations) in much the same way that tanks did in the First World War and the atomic bomb in the second [5-11, 13-17].

It should be specially noted that with the massive introduction of information technology and the use of information weapons, the goal of the war was not the destruction of the enemy, but their management. In other words, information technology in our time has made it possible to "control the enemy" with minimal violence and bloodshed.

The task of suppressing the enemy now consists not in destroying the living force, but in undermining the world outlook of the population, in destroying the infrastructure of the state, including the armed forces, in undermining the authority of its leaders. This is proved by the results of the recent military operations of the United States and NATO countries in Iraq, Yugoslavia, the aggression of the Russian Federation against Ukraine in the Donbass, as well as its annexation of Crimea [18].

Final formulation of the concept of information warfare has not yet taken shape. Martin Libiki from the US National Defense University on this occasion spoke thus: "attempts to fully understand all the facets of the concept of information warfare reminiscent of the efforts of the blind, trying to understand the nature of an elephant: one who touches his leg, calls it a tree; the one who feels the tail, calls him a rope and so on. Is it possible so to get the right idea? Perhaps there is no elephant and there, and there are only trees and ropes.

Some are ready to be brought under this concept too much, while others treat some aspect of information warfare as a concept in general."

Information warfare is a comprehensive, coherent strategy for the implementation of information and psychological impact on the enemy, due to the increasing importance and value of information in matters of command, control and policy. Information warfare involves coordinated activity on the use of information on the one hand information processes and systems as the object of influence, and on the other - as a weapon for fighting in the military, political, economic and social spheres [5-13].

The goal of information warfare is to ensure national security through information and psychological impact on the opposing side and protecting their own information resources.

By its nature, information warfare occupies a position between the "cold" war (including, in particular, economic) and actual combat with the participation of armed forces.

Unlike economic war information warfare result is a malfunction enemy infrastructure elements (control points, and rocket launch sites, airports, ports, communication systems, warehouses, etc.), and with conventional weapons in contrast to the "hot" war and (or) weapons of mass destruction of its objectives are not material, and the "ideal" (informational) objects or material carriers. At the same time the destruction of such facilities and systems can be performed with preservation of their material basis.

According to The US Army's Field Manual information warfare is defined as actions aimed at achieving information superiority in the interests of national security, carried out by influencing the information, information processes and information systems of the enemy while protecting own information, information processes and systems [14].

Since the information war is directly connected with information processes, it can be said that information warfare is a war for knowledge about oneself and the enemy.

The information war is being waged on two main levels: the state and the military.

For each of these levels can be distinguished relevant organs, methods, tools, and objects of exposure. The goal of information warfare is achieved by conduction of offensive and defensive actions.

Offensive activities aimed at establishing control over the enemy's control systems or their destruction and may be held in secret or openly.

Defensive measures serve to protect their own information resources from enemy action.

As an evidence that the information war is not a slogan and not a myth but an objective reality, the US Department of Defense adopted guidelines and handed out the structure of organs of information warfare [14-19].

Relevant documents for all kinds of armed forces has been developed and adopted. These documents secured certain responsibilities for officials of the armed forces management system.

Information war in the US Armed Forces in practice, primarily carried out by: Chairman of the Joint Chiefs of Staff and the two departments, specially created joint headquarters; commanders of unified commands US forces in the region; Commander of the Joint Special Operations Command; Head of the National Security Agency; Chief of Defense Intelligence Control; Head of the Department of Defense information systems; chiefs of armed services staffs.

The faculty on information counteraction has been created in the National University of Defense of Ukraine named after Ivan Chernyakhovsky to train

specialists, its graduates are trained in the entire range of issues related to the information warfare: from protection against computer attacks to supporting the planning of military operations.

Today, each armed service of the US Armed Forces has its own specialized center. Tasks of the US forces Center of Information fighting, for example, are:

the creation of means of information warfare in support of armed services operations;

planning a campaign,

acquisition and testing equipment,

protection from the armed services staffs an information attack.

To this end, the Center educates, equips and deploys response team, develops and maintains database and application software, analyzes the vulnerability of electronic systems. Due to efforts of the Center's employees created a "Distributed Intrusion Detection System" that identifies abusive computer systems, monitors user activities, provides centralized access to information about the security status of a particular system, and distributes the processing of verified data.

Preparing to conduct information warfare in the United States is conducted in three areas: in the armed forces, the security services and nationwide.

In the armed forces preparing for information war involves theoretical, organizational and logistical arrangements. In the army, the navy and armed services created positions for officers dealing with these issues. The military schools hosting games and training on improvement of curricula. And finally, the most important thing is that the US military heavily equipped with means of information warfare, spending on the purchase of information technology more than a nuclear and space programs.

The security services conducted not less intensive work. National Security Agency creates a sudden "infected" computers and computer systems, as well as various schemes of "bookmarks" for computer viruses and logic bombs. The CIA training is conducted in two programs. The first program includes the introduction of a system of military-industrial complex in peacetime easily triggered at the right time, logic bombs, and viruses. The second program is aimed at developing ways to influence the programmers working on defense enterprises, in order to attract them to infiltration of viruses and logic bombs in the information systems of enterprises in crisis situations.

Preparation for information warfare at the national level is to improve the national information infrastructure, including information systems, banking, communications, transport, energy, industry and services. The increasing importance of this structure is the Internet.

Let's consider the basic ways of conducting information wars.

US concept of information warfare is assumed that in peacetime, information warfare is conducted secretly, but if non-military actions can not achieve the desired goals, the military force may be used. Thus, the operations were held in Panama, Grenada, Iraq, and Yugoslavia. In wartime, the information war will be open and combined with traditional methods of warfare.

There are a number of possible reasons why the enemy can stop the fighting:

1) Inability to control the armed forces;

2) Demoralization of the armed forces or the population as a whole;

3) Obtaining information (real or alleged) that the army destroyed, or that is more advantageous to stop the war, than to continue to fight.

Information warfare involves the use of complex methods of state and military levels.

At the military level, one can distinguish five ways of information warfare which are combined under the operational-strategic US military concept of "struggle with control systems":

1) Psychological struggle;

2) Mislead the enemy or deception;

3) Countering enemy reconnaissance;

4) Electronic Warfare;

5) Destruction of command centers and communications systems.

The main objects of the information war impact are:

1) General public (civilians and military personnel), its state, economic, and social institutions;

2) Different levels of controls (from the highest to the lowest governing body);

3) Information infrastructure of the state and the armed forces;

4) The media.

Each of these facilities covers broad areas of the state and its security. For example, there are strikes of vital elements such as telecommunications and transportation systems when exposed to a state and military information infrastructure. Similar actions can be taken by geopolitical or economic opponents or terrorist groups.

Let's consider the basic spheres of a society vital activity, the state which are subject to threats of information security (fig. 1).

There are advantages against the enemy by means of information warfare:

the ability to selectively influence a predetermined time at a strictly definite element management system;

relatively low cost of development, methods and means of conducting;

lack of boundaries in relation to the development and integration of the information infrastructure of various countries;

inability to define clearly the beginning of information warfare;

high vulnerability information systems.

The methods of information warfare can also be divided into direct and indirect. The difference between them can be illustrated by the example R. Shafraniki. Let’s say the aim is to make your opponent believe that the regiment is located where it

is not present, and act on this information in a manner that is beneficial to us.

An example of an indirect method of information warfare that is using engineering tools to build models of aircraft and false airfield facilities, as well as to simulate the activity of working with them. In this case, the impact will be successful if the opponent will be watching the wrong airport and consider it real.

Direct way of information warfare that is the direct creation of false records in the regiment of the enemy information storage. In case of success of such an impact, the result will be the same as in the first case, but the funds involved to obtain this result, to be materially different.

Another example of a direct way of information warfare can be a change in the information in the enemy database on existing communications during operations (making false information that the bridges are broken) to isolate individual enemy units. This can be achieved by bombardment of bridges. And in fact, and in another case the enemy, making a decision based on the information available, to take the same decision that is to produce a movement of troops through other communications.

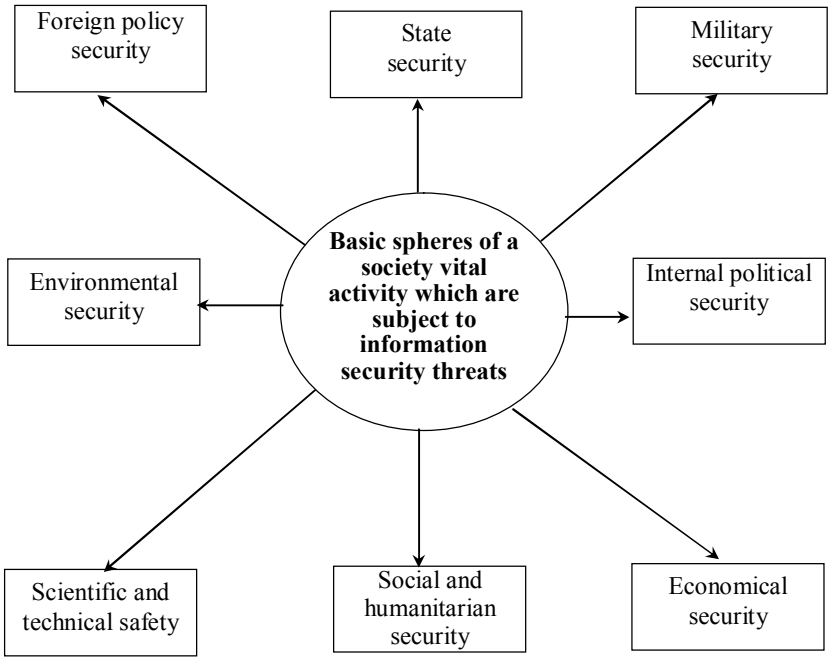

Fig. 1. Basic spheres of a society vital activity which are subject to information security threats

The main directions of management systems threat during information warfare.

Let's outline the following main areas of threats to control systems, in particular, military command and control systems, in information warfare:

1) advance by the control cycle;

2) technological superiority in the management and communication means;

3) expansion in the market of automated control and communications;

4) information superiority;

5) superiority in offensive information warfare means.

In the first direction, a significant advance over the management cycle is carried out by creating a new information infrastructure of the armed forces, which should provide a fundamentally new level of the functioning of the command and control organs, allowing to significantly outstrip the enemy in organizing and conducting military operations at any level and anywhere in the world.

A key role in the new information infrastructure will play a single for all armed forces complex of DoD information systems. His work with the sources and users of information should be carried out through the Internet and a unified information network DoD, as well as tactical and tactical communication systems, data distribution, targeting and navigation.

The second direction is that to achieve a significant technological superiority in the field of command and control and communication tools. US achieving technological superiority leads to gradual displacement of domestic communications frequency spatial and temporal domains. For example, the use of complex structure in the radio signals project "Speak easy" allows to secure exchange of information at high speed even in the range in excess of HF interference power over the useful signal of hundreds or more times.

The high data transfer rate, high-quality and reliable communication channels enable timing advance of national control systems. Creating a global communications and information systems and bring it to the tactical level gives an advantage in the conduct of the war on unprepared in terms of communication area. The third area is that a large-scale expansion in the area of management and communication tools, caused by the fact that in Russia, unlike other European countries, there is no strict measures to limit the introduction of alien systems in the state's

information infrastructure. Currently, for foreign companies Russia is one of the cheapest and most powerful polygon to simulate mobile technologies. You can hold any approbation, including to introduce "dead-end" system.

Weak control over the use of the radio spectrum can deliver the Ukrainian Armed Forces in a vulnerable position in terms of the organization of communication and security. Having access of foreign operators to the system switch allows them to detect, report and transmit to the US Defense Intelligence Agency and the FBI data on all the interests of cellular communication network subscribers.

One of the ways to reduce the efficiency of material and intellectual resources of the state and its armed forces is delivering of low-cost automation and communication equipment, the organization of information targeted diversion and technological materials.

The fourth area is related to the achievement of information superiority. This direction intersects with the first and second directions. Information superiority is ensured by three components:

1) reconnaissance conduction on a global scale, efficient reception, processing and transmission of information;

2) protection of its information resources and information technologies;

3) destructive action to suppress the enemy's capabilities to develop its own technology and the information acquisition.

According to the US Department of Defense believe that in order to achieve victory in the armed conflicts of the new century, it is first of all necessary to promptly receive, process and transmit information. The one who can quickly gather information about the conduct of operations (combat operations) will win, analyze them, draw the right conclusions, make the right decision and quickly bring it to subordinates.

It is necessary to obtain information superiority to ensure victory over the enemy. It allows you to get ahead of the enemy in the understanding of the rapidly changing situation in the conduct of operations (combat operations), to make decisions proactively, and to design the right course of the battle.

The concept of information superiority is based on the concept of space conducting operations or battle space, which allows you to evaluate the military conflict in its entirety.

Operations space includes not only information about specific areas where battles are conducted, but also data on the system of logistics, the work of all levels of command, on the political aspects, and many other things that are directly or indirectly related to the war.

One will have information superiority who better, faster and more accurately able to get a description of the conduct of operations of the space. This allows to apply the necessary force at the right time in the right place, which is known to decide the outcome of any battle or even allows you to win without bloodshed. One who has information superiority will be ahead of the opponent in the accuracy of orders and, most importantly, in the promptness of their delivery. Units will operate synchronously and be able to react quickly to changing circumstances.

The US military distinguishes the following areas of using information superiority.

1. Commanders are able to carry out a synchronous proactive maneuver with strikes against key targets by receiving promptly processed information about the location and condition of each unit in the zone of operations and the most important enemy facilities.

2. It becomes important to identify the most important facilities for the destruction and capture in carrying out the attack. These objects are automatically ranked using a variety of algorithms and rules implemented by using expert systems.

3. Information superiority makes it possible to organize multi-faceted defense without fear of an unexpected attack by the enemy. Defense issues are particularly important during the deployment of forces and maneuvers, when the troops are most vulnerable. The success of synchronous maneuvers, including the pre-planned joint actions of various types of troops, largely depends on the combat readiness of all units at the time of arrival to the battlefield. Therefore, it is necessary to ensure their safety in order to maintain maximum efficiency and the ability to operate freely in the zone of operations.

4. It is impossible to count on the success of conducting operations (combat operations) without the organization of targeted material and technical supply. The targeted material and technical supply is based on continuously incoming information from the operations zone and allows, with the help of various technologies for the delivery of appropriate resources, to maintain the combat readiness of military equipment in all conditions of the surrounding area at the required level.

The use of a network of focal points of the Federal Bureau of Investigation analyzing information coming from virtually the entire territory of the globe and issuing daily press releases to state and military authorities in the military-political setting (indicating the actions of troops of foreign states up to a separate military unit or ship) is a clear example of conducting reconnaissance on a global scale.

In addition, these focal points form press releases of the appropriate focus for psychological impact.

The fifth area is to achieve excellence in the information warfare offensive weapons field.

It is necessary to clearly identify the sources of information warfare. Information warfare can be started immediately, without special training, with a massive use of various media information warfare. It does not require preliminary transfer, concentration, and act instantly by commands or from satellites, or from remote control panels remote from targets, or by signals from portable consoles of special agents.

Means of information warfare. Theorists often refer to the means of information warfare to the so-called information weapon, which means a wide class

of means of information influence on the enemy: means of disinformation and propaganda; means of electronic warfare; means of destruction, distortion or theft of information arrays; means of overcoming protection systems; means of limiting the admission of legitimate users; means of disorganization of the work of technical means, computer systems and communication systems, etc.

The purpose of the means of information warfare is to influence the information, information processes and information systems of the enemy to undermine his economy, reduce the degree of combat readiness. At the same time, it means that information warfare can be fought as independently, ie. without the use of traditional means and methods of armed struggle, but in combination with other means and methods of conducting operations (combat operations).

The main means of information warfare. The arsenal of information warfare is large enough. According to the content of the events they can be defensive and offensive. Defensive means are intended to protect information, information processes and systems, preventing the enemy from conducting a successful information attack. These means ensure the implementation of actions to prevent and detect information actions of the enemy, as well as the organization of counteractions.

Defensive means include four large groups:

1) means of a new information infrastructure (a complex of information systems of the Ministry of Defense, the Internet, an integrated information network of the Ministry of Defense, tactical and operational-tactical communication systems, targeting, guidance and navigation, a complex of information storage and processing facilities, information infrastructure management tools);

2) means of ensuring the security of the information infrastructure (means of protecting communication channels, territories, premises, devices, means of operating systems protection, databases, software, encryption means, access control facilities, etc.);

3) means of information support (radio electronic reconnaissance, space reconnaissance, aerial reconnaissance, intelligence reconnaissance, reconnaissance by technical means);

4) means of information-psychological influence (television, radio, print, etc.).

Offensive means of information warfare on the area of their impact can also be grouped into four groups:

1) means of information-psychological impact, which have a psychological effect on the psyche of people and allow them to control their behavior. The resources of this group can be used to solve both offensive and defensive tasks;

2) means of information impact, allowing to receive, transform and transmit critical information, for example, misinform the enemy's personnel;

3) means of active influence that allow to disrupt the functioning of information systems that ensure the functioning of state, military, industry, transport, communication, energy, banks and other agencies' control bodies through information impact;

4) means of impact and fire damage.

Consider a few examples of means of information influence.

First, the already widely used Pentagon satellites, spy planes and unmanned aircraft to track the ground enemy should be mentioned. In the future, thousands of tiny sensors can be dropped from aircraft or hidden on the surface of the Earth.

As a means of informational impact, “Raytheon” developed a device for intercepting information and introducing misinformation, which breaks the intercepted message into segments and combines them in the necessary way to create a new message. This device makes it possible to accumulate data on specific individuals for a long time, to form and transmit false messages in their voice. This is especially important for the tactical link, where every soldier must constantly hear the voice of his commander.

There are thrown unattended information sensors in the arsenal of information warfare authorities. They allow to enter false messages into those communication channels to which there is no direct electromagnetic access.

Means of processing and transferring images find a widespread use to influence the psyche of computer operators. They use the effect of the "25th frame" and special images that paralyze human activity. During the US military exercises in Somalia, the effect of a holographic image of Jesus Christ against a background of a cloud of sand and dust was used. This allowed for a long time to paralyze the actions of personnel. According to the conclusion of the US military experts, the psychotropic losses of Iraqis during Operation Desert Storm greatly surpassed the physical.

A prototype of the "21st century infantry ammunition" was created, and its helmet is equipped with a microphone and headphones, night vision goggles and video terminal sensors, as well as an eye level display that will display the battlefield image from a bird's eye view and constantly updated intelligence data.

It is necessary to emphasize the enormous importance of the Internet for solving both the offensive and defensive tasks of the information war.

The Internet has two important and dangerous properties: survivability and the ability to arbitrarily connect to military control networks of military objects of strategic importance (if they have an "exit" to the Internet).

During the war in the Persian Gulf, the United States, despite its powerful information impact, was never able to completely isolate Iraq from the outside world.

The government of Iraq bought the weapons through the Internet, listing money suppliers stored in foreign banks. So the Americans created, as they say, on their own head, a network that is resistant to "partial damage".

The prevalence of electronic automation of federal services and agencies in the United States creates the conditions for "computer espionage" and information diversions, yet the US continues to develop the national information infrastructure, subordinating it to the idea of American leadership in the world. Information weapons, created in the United States as a result of a major technological breakthrough, fully contributes to its materialization in the foreseeable future.

In view of inherited information isolation and technological backwardness, Ukraine is, of course, less vulnerable than advanced countries such as the United States, Germany and Japan. However, a high degree of centralization of the structures of state management of the Ukrainian economy can lead to disastrous consequences as a result of information impact.

Of course, our special services have the necessary means and know-how to prevent interception, leakage, distortion, destruction of information in information and telecommunications networks and national systems, but the pace of improving information weapons (as well as any type of attacking weapons) exceeds the rate of development of protection technologies. That is why the tasks of timely detection of the impact of information weapons and neutralization of its manifestation should be considered as priority tasks in ensuring national security of the country.

Conclusion from this explosion

In this article, the authors analyzed the impact of information counteraction on the organization of managerial activities of officials.

It is established that the use of modern information technologies as one of the means of armed struggle led to changes in the strategy and tactics of conducting modern wars and military conflicts.

The military-political leadership of many countries of the world developed the concepts of conducting information wars, taking into account the factors of information vulnerability of the warring parties. practical implementation of these concepts is carried out by conducting information (information-psychological) operations.

The analysis of the views of the military-political leadership of some developed states of the world on information warfare showed that it has two components:

information and technical (information operations);

information-psychological (information-psychological operations).

The effectiveness of information warfare in the military sphere, in many respects, depends on the efficiency, purposefulness, continuity and clarity in its organization and management.

For this purpose, an information security system should be established, which the main tasks are:

- forecasting of potential threats to information security, their detection and on this basis forecasting changes in information security;
- implementation of a set of appropriate measures to prevent and eliminate them;
- creation and maintenance of information security resources and means in the readiness for their application.

As a result of the research conducted by the authors of this article, it is proposed to adjust the normative documents in order to take into account additional destructive factors for the organization of managerial activities of officials, namely, information counteraction, and also proposes to change the management training system in order to train the latter to make correct and deliberate decisions in conditions information confrontation.

The direction of further research should be considered the development of the officials activities dynamic model in the context of information resistance.

REFERENCES

1. Pyevtsov, G.V., Zalkin, S.V., Sidchenko, S.O. and Khudarkovsky, K.I. (2014), *Informational security in the military sphere: problems, methodology, system of protection*, Digital printing house, Kharkiv, No. 1, 272 p.
2. Manachinsky, A. (2000), *The Third World War: information war*, Man and the law, Kyiv, No. 3 (4), 41 p.
3. Rusnak, I.S. and Telelim, V.M. (2000), "Development of forms and methods of conducting information struggle at the present stage", *Science and Defense*, Kyiv, No. 2, pp. 18-23.
4. Tolubko, V.B. (2003), *Information struggle (conceptual, theoretical, technological aspects),* monograph, NUDU, Kyiv, 320 p.
5. Tolubko, V.B., Zhuk, S.Yu. and Kosevtsov, V.O. (2004), "Conceptual Foundations of Information Security of Ukraine", *Science and Defense*, Kyiv, No. 2., pp. 19-25.
6. Sidchenko, S.A., Khudarkovsky, K.I and Petrov, V.L. (2004), "Information protection weapons as a new class of weapons in the conduct of information defensive operations", *Information processing systems*, Kharkiv Military University, Kharkiv, No. 11 (39), P. 163-169.
7. Bryukhovsky, G.N., Krylov, G.O. and Turko, N.I. (2000), *Fundamentals of Information Security state at the present stage*, Military academy of the general staff, Moscow, 68 p.
8. Kovtunenko, O.P., Bogucharsky, V.V., Slyusar, V.I. and Fedorov, P.M. (2006), *Weapons on non-traditional principles of action (state, trends, principles of action and protection from it): monograph*, Publishing house Poltava military institute of signal communication, Poltava, 248 p.
9. Pevtsov, G.V. and Cherkasov, O.L. (2008), *Providing information security of the region: problem, concept and ways of its realization*, KRI NAPA "Magister" Publishing House, Kharkiv, 136 p.

10. Kotenko, I.V. (2000), *Legislative-legal and organizational-technical support of information security of automated systems and information networks*, Military Academy of Communications, St. Petersburg, 190 p.
11. Kotenko, I.V. (1998), *Theory and practice of constructing automated information and computing support systems for communication planning processes based on new information technologies,* Military Academy of Communications, St. Petersburg, 404 p.
12. Forbes, A. and Henley, D. (2012), *The Illustrated Art of War: Sun Tzu*, Chiang Mai: Cognoscenti Books. ASIN: B00B91XX8U.
13. Kovalevsky, S.S. (2006), "Information security of the Russian Federation and the current state of informatization of public authorities", *Academy of Trinitarianism*, Moscow, El. No. 776567, pub. 13296.11.05.2006.
14. FM 3-05.30. Psychological Operations. 19 June 2000.
15. FM 3-05.20. Special Forces Operations. 26 June 2001.
16. JP 3-13. Joint Doctrine for Information Operations. 9 October 1998.
17. JP 3-57. Joint Doctrine for Civil-Military Operations. 8 February 2001.
18. Pevtsov, G.V., Zalkin, S.V., Sidchenko, S.O., Khudarkovsky, K.I. and Gordienko, A.M (2015), "Analysis of the structure, functions and tasks of the information and psychological control bodies in the armed forces of the world leading countries", *Science and technology of the Air Forces of the Armed Forces of Ukraine*, Kharkiv, No. 3, pp. 37-46.
19. Levchenko, O.V. (2015), "Conceptual approach to the comprehensive assessment of the information security state", *Science and technology of the Air Forces of the Armed Forces of Ukraine*, Kharkiv, No. 3, pp. 47-50.
20. Kosogov, O.M. (2015), "Methodological approach to the analysis of threats to the state's information security in the military sphere and the definition of counteraction measures to them", *Science and technology of the Air Forces of the Armed Forces of Ukraine*, Kharkiv, No. 3, pp. 51-53.

Надійшла (received) 23.02.2018
Прийнята до друку (accepted for publication) 25.04.2018

Аналіз впливу інформаційної протидії на організацію управлінської діяльності посадових осіб

Д. О. Кисіль, О. Ф. Сальнікова, С. І. Антоненко, А. В. Шишацький

У зв'язку зі збільшенням активності використання сучасних інформаційних технологій як одного із засобів збройної боротьби змінилася стратегія і тактика ведення сучасних війн і військових конфліктів. З цією метою авторами даної статті було розглянуто поняття інформаційної протидії та його вплив на організацію управлінської діяльності посадових осіб. В ході проведення дослідження встановлено, що керівництвом багатьох країн світу розроблені концепції ведення інформаційних війн, що враховують фактори інформаційної вразливості протиборчих сторін, практична реалізація цих концепцій здійснюється шляхом проведення інформаційних (інформаційно-психологічних) операцій. Проведений аналіз поглядів військово-політичного керівництва деяких розвинених держав світу на ведення інформаційної боротьби показав, що вона має дві складові: інформаційно-технічну (інформаційні операції) і інформаційно-психологічну (інформаційно-психологічні операції). В результаті проведеного дослідження авторами даної статті пропонується провести коригування нормативних документів з метою урахування додаткових деструктивних чинників на організацію управлінської діяльності посадових осіб, а саме інформаційного протидії. Також авторами статті запропоновано змінити систему підготовки управлінської ланки, з метою навчання останніх приймати коректні і обдумані рішення в умовах інформаційного протистояння.

Ключові слова: інформаційне протистояння; управління; прийняття рішення; інформаційні технології; інформаційна війна.

Анализ влияния информационного противодействия на организацию управленческой деятельности должностных лиц

Д. А. Кисель, О. Ф. Сальникова, С. И. Антоненко, А. В. Шишацкий

В связи с увеличением активности использование современных информационных технологий как одного из средств вооруженной борьбы изменилась стратегия и тактики ведения современных войн и военных конфликтов. С этой целью авторами данной статьи было рассмотрено понятие информационного противодействия и его влияние на организацию управленческой деятельности должностных лиц. В ходе проведения исследования установлено, что руководством многих стран мира разработаны концепции ведения информационных войн, учитывающие факторы информационной уязвимости противоборствующих сторон, практическая реализация этих концепций осуществляется путем проведения информационных (информационно-психологических) операций. Проведенный анализ взглядов военно-политического руководства некоторых развитых государств мира на ведения информационной борьбы показал, что она имеет две составляющие: информационно-техническую (информационные операции) и информационно-психологическую (информационно-психологические операции). В результате проведённого исследования авторами данной статьи предлагается провести корректировку нормативных документов с целью учёта дополнительных деструктивных факторов на организацию управленческой деятельности должностных лиц, а именно информационного противодействия. Также авторами статьи предложено изменить систему подготовки управленческого звена с целью обучения последних принимать корректные и обдуманные решения в условиях информационного противостояния.

Ключевые слова: информационное противостояние; управление; принятие решения; информационные технологии; информационная война.