УДК 004.05(075.8)
Луцький національний технічний університет[1)]
Університет Бєльсько-Бяли, Польща[2)]
І.Є.Андрущак[1)], І.В.Андрощук[1)], В.П. Марценюк[2)]

ТЕХНОЛОГІЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ.

І.Є.Андрущак, І.В.Андрощук, В.П. Марценюк. Технології кібернетичної безпеки інформаційних систем. У статті розкривається основні поняття і зміст сучасної кібернетичної безпеки. Визначається її роль і значення для інформаційної сфери.
Ключові слова: безпека, кібернетична безпека, інформаційна безпека.

И.Е.Андрущак, И.В.Андрощук, В.П. Марценюк. Технологии кибернетической безопасности информационных систем. В статье раскрывается основные понятие и содержание современной кибернетической безопасности. Определяется ее роль и значение для информационной сферы.
Ключевые слова: безопасность, кибернетическая безопасность, информационная безопасность.

I.Ye.Andrushchak, I.V.Androshchuk, V.P. Martsenyuk. Technology of cybernetic security information systems. The article reveals the basic concept and content of modern cybernetic security. It determines its role and significance for the information sphere.
Key words: safety, cybernetic security, information security.

Formulation of the problem. The development of the information sphere of Ukraine opens not only new opportunities for the person, state and society, but also puts new, ever more complex tasks that require an objective and timely solution. The evolution of information relations requires revision and updating of existing legal rules of the actors as the main means of their settlement. The right should promptly react to any changes in social relations, otherwise its regulatory impact will be reduced, which will lead to negative consequences.

In connection with this, constant monitoring and evaluation of certain phenomena arising in the state and social life is necessary, in order to ensure, based on the experience gained, the modernity and relevance of legal norms.

So, for example, increasingly in daily life, scientific, analytical and news articles devoted to the development of information technologies, we encounter the terms "cyberspace", "cybercrime", "cyberwar", "cyberterrorism" and the like. However, if you turn to legal norms, then, unlike the sources, they do not abound by such terms.

Setting up tasks. Do they symbolize a new stage in the development of information relations, or is it just a game of words, in order to attract the attention of the public? What relation do they have to the modern problems of the information sphere, military security and to science derivatives, from which name they are?

Cybernetics (from Greek kybernetike - art of management) is the science of the general laws of obtaining, storing, transmitting and processing information. The main object of the study is the so-called cybernetic systems, which are considered abstract, regardless of their material nature. Each such system is a set of interconnected objects (elements of the system) that can perceive, memorize and process information, and exchange it. Cybernetics develops general principles for the creation of control systems and systems for the automation of mental labor. The main technical means for solving the problems of cybernetics are computers. Therefore, the emergence of cybernetics as an independent science is associated with the creation in the 40's. 20th century these machines, and the development of cybernetics in the theoretical and practical aspects with the progress of electronic computing.

As can be seen from the original concept of cybernetics is the concept of management. Under the control of the broad sense of the word, the ordering of the control system is understood, i.e. bringing this system in line with the laws of the surrounding objective reality. Since such an interpretation of the concept of control extends it to objects of inorganic nature, obeying physical laws, the concept of management of a number of authors extends only to living systems and artificial control systems (computers, etc.).

Analysis of recent researches and publications. Not surprisingly, in the modern period of the formation and development of world information civilization, the large-scale penetration of information technologies, the importance of cybernetics also increases. If earlier computers and related technologies were not widespread, now they are present everywhere, with their application built control systems for different purposes, composition and level.

A large number of scientific works reflecting different views on their nature and relationship are devoted to the study of phenomena of information and management. However, the fact that control without information is impossible is not disputed by anyone. Information acts as an integral resource of management.

The control system consists of two blocks - a control system and a controlled object connected by direct and reverse links. The control system transmits a control effect on the control object through the direct link channel. Information about the state of the control object is transmitted to the control system through the feedback channel.

In essence, management is the organized exchange of information between elements of the system in order to maintain them in a certain state. However, if any kind of management uses information, then far from any information is suitable for management.

In order to carry out the management process, it is first of all necessary to obtain information about the controlled object and bring it into a form suitable for communication over the channels. After bringing the information into this form, it is transferred to the control system (in which the computer or human brain can act as a computer). The management system, having processed the received information on the basis of the rules laid down in it, develops management commands and passes them to the executive bodies, which, acting on the control object, change the state of the latter. Further, information about actions performed by the executive bodies, the status of the control object and external influences through the feedback channels is transferred to the control system, which uses this information to generate new control commands.

Consequently, there are the following universal components of the control process:

- management information - a specific type of data necessary for the management to be carried out, including: data on the controlled object, its condition, external influences, actions executed by the executive bodies, control commands;
- control forces - its implementing entities (management system), executive bodies;
- management means - communication and feedback channels, as well as management information management tools (management infrastructure);
- order or control algorithm - the rules on the basis of which the control system processes information and develops management commands.

The nature of these components coincides with the nature of the elements of the information sphere, which includes: information, information infrastructure, subjects of information relations and the system of their regulation. Based on this, management information is a specific type of information, management infrastructure is a kind of information infrastructure, and subjects of management are the kind of subjects of information relations.

Of particular interest is the comparison of such elements as the order (management algorithm) and the system of regulation of information relations. On the one hand, in the context of the elemental comparison they have, they have a similar nature and purpose - they are the basis of the formation of a controlling influence.

However, on the other hand, if the management (management algorithm) is a set of rules for processing information and elaborating management commands, then the system of regulation of information relations includes not only such rules. It also includes management information (the data on which management decisions are made) and management entities, in the role of which are state authorities and their officials authorized in the field of information relations regulation, and the corresponding infrastructure.

Basic material presentation. The system of regulation of information relations is a concrete example of a cybernetic system, and information relations act as the object of its management.

In turn, the foregoing makes it possible to conclude that within the information sphere there is a cybernetic sphere (cyber sphere) - a management sphere that includes a special type of information, subjects, infrastructure and rules necessary for the implementation of the management process.

In addition to the inextricable link between the information sphere and the cyberspace, they become apparent and the differences between their elements make it possible to differentiate existing threats against them and, consequently, also take these features into account when securing management safety.

If the provision of information security is an activity aimed at achieving a state of security of the information sphere in which implementation of known threats against it is impossible, the provision of cybernetic security is an activity aimed at achieving a state of security of management, in which it is not possible to violate it.

In addition, providing information security is an easily scalable category, the features of an object or system within which it is implemented, does not fundamentally affect its content. This activity includes ensuring the safety of information, information infrastructure, subjects and the system of information relations regulation both on a state scale and on a scale of a separate organization.

In the case of cybernetic security, the situation is somewhat different. Its security is now more dependent on the features of the cybernetic system and management processes, since various requirements are subject to different requirements that must be observed.

For example, if it is necessary to ensure, in relation to public administration,, among other things, that citizens should be informed about the activities of the authorities, that is, their openness and the availability of relevant information. In relation to, for example, the control of troops on the contrary, it is necessary to ensure its stealth.

In addition, due to the widespread use of information technology in the military sphere, along with the classical requirements for a management system (sustainability, continuity, efficiency, stealth, efficiency) today, there are fundamentally new requirements, such as:

- adaptability to changing conditions and methods of using the Armed Forces;
- ensuring a single information space on the battlefield;
- openness in terms of constructing and expanding opportunities;
- ability to reduce operational and maintenance personnel;
- evolution in development;
- technological independence;

Thus, the maintenance content of cybernetic security can vary significantly depending on the requirements imposed on the control system, its purpose, the specifics of the controlled object, the environment conditions, the composition and condition of the forces and means of management, as well as the order of management.

What, in general, is it necessary to distinguish information and cybernetic security? What tasks can be solved with such a delimitation? Such a necessity determines the transition to a new socioeconomic formation, called the information society.

If earlier problems of cybernetic security were relevant mainly to the military organization, in connection with the existence and development of the forces and means of information confrontation and radio-electronic struggle, now such problems exist in relation to the state as a whole.

Thus, the tasks of providing cybernetic security to date exist, both in relation to the state as a whole and in relation to certain critical structures, systems and objects.

Let's consider in more detail some of these reasons, which necessitate the separation of cybernetic security as an independent form of security.

One of the new negative phenomena posing a danger to the information sphere is the emergence of hacker groups occupying an active social position and covering their activities in social networks and mass media. Unlike classical hacker groups who seek not only to conceal their activities, but also the very fact of their existence, the so-called hacktivists position themselves as fighters with injustice and arbitrariness, and follow certain rules and principles independently elaborated. Moreover, an analysis of the activities of such groups makes it possible to conclude that they pursue non-commercial goals. In their activities, ideological (political), and not material motivation prevails, which makes them a more serious threat to the state and commercial companies, as compared to ordinary criminals.

These facts allow us to conclude that part of the hacker community has become interested in the political and economic situation and is trying to influence it by organizing and holding mass protests and massive hacker attacks on the resources of the state, including military and commercial structures. The existence of such groups, their ideology and political motivation, the negative attitude of their members to the state authorities and the neglect of established law and order, present a real danger to the state, including military administration and its infrastructure.

Many experts in information security call hacktivism one of the main negative trends of the past and the coming years. Taking into account the fact that the activities of such groups are transboundary and expressed in the conduct of illegal actions in the information space, it is also a threat to the information sphere of Ukraine.

Another example of the need to allocate cybernetic security as a separate category is the work of foreign countries to create special units and structures whose names speak for themselves. Recently, in a number of states, so-called centers of cybernetic defense (defense) appeared. Such centers in one form or another already exist in the USA, UK, Australia, Israel, Iran, China, Germany.

In general, the tasks of such units are roughly the same in all countries - together with special services and law enforcement agencies, they protect public authorities, as well as civilian and military

critical objects from harmful effects (hacker attacks, malware, etc.). However, their very name, purpose, main tasks and affiliation, in most cases, to the military organization, indicate the priority of the goals of ensuring the security of state and military management.

For information conflicts, special information-shock groups of forces and means are created, the purposes of which are, as a rule, to be: neutralization or destruction of the information and strategic resource of another (controversial) subject and its armed forces and ensuring the protection of its information-strategic resource from a similar impact the enemy As the main objects of influence for these forces and means specify:

- software and information support;
- software-hardware, telecommunication and other means of information and management;
- communication channels, providing circulation of information flows and integration of the control system;
- human intellect and mass consciousness.

Emphasizing the special importance of the information sphere and its related processes for the defense of the state, the author identifies military information security as one of the types of military security.

Recently, the attitude towards information confrontation has changed considerably, it is no longer perceived merely as an activity contributing to military operations. More and more factors make us treat it as an independent and most promising form of negative influence on the enemy.

In its new quality, such an impact is not only beyond the limits of classical warfare, but also gets broader content. It becomes a powerful, invisible and unforeseen international law, a means which allows, in the shortest possible time, to paralyze the main forces and means of a hostile state without causing fatal damage to its industrial sites and territories.

That is why it is necessary to further develop relevant developments in the military science and their application not only within the framework of the military organization, but also the entire information sphere of Ukraine. The current situation and the specifics of new threats erode the boundaries between peace and wartime and require the constant participation of all forces and means of the state in ensuring its information security.

To achieve these goals, full consolidation of efforts and a clear interaction between law enforcement agencies, special services, military units, research organizations, mass media, public associations and commercial companies are needed.

Particular attention deserves attention to the problem of inconsistency of the legal basis, both international and domestic, with modern information relations, its inability to take into account the danger of new negative phenomena threatening the information sphere as a whole and its individual elements.

Based on this, encroachment on the object of a critical infrastructure implemented through the use of information technology, in addition to all its advantages associated with high latency and anonymity, has one more - provides for less severe punishment.

At the same time, within the framework of the Military Doctrine of Ukraine among the main internal military threats, disorganization of the functioning of state authorities, important state, military objects and information infrastructure of Ukraine is indicated. One of the main military threats is the obstruction of the functioning of the state and military management systems of Ukraine, the disruption of its strategic nuclear forces, missile warning systems, space control, nuclear weapon storage facilities, nuclear energy, nuclear, chemical and other potentially hazardous ones objects.

It is also noted that military conflicts will be characterized by the speed, selectivity and high degree of damage to objects, the speed of maneuver by troops (forces) and fire, the use of various mobile groupings of troops (forces). The mastery of a strategic initiative, the preservation of sustainable state and military governance, the provision of superiority on land, the sea and in the air and space will be decisive factors in achieving the goals set.

Within the framework of the National Security Strategy of Ukraine until 2020 it is noted that the negative impact on the state of military security of Ukraine and its allies is exacerbated by the abandonment of international agreements in the area of arms limitation and reduction, as well as actions aimed at breaking the stability of state and military management systems, warning of missile attack, space control, the functioning of strategic nuclear forces, nuclear weapon storage facilities, nuclear power industrialists, nuclear and chemical industry, other potentially dangerous objects.

It turns out that the legislator can no longer be blamed for not knowing the situation or ignoring these threats, even in the context of providing military security. Within the framework of the mentioned documents, special attention is paid to the threats connected with the information sphere, state and military administration. However, the question arises - why is the matter limited only to their transfer, and

on this use of the potential of legal regulation ends? After all, the modern legal framework can have a decisive impact on the security of the information sphere and minimize the risk of exposure to threats.

There are no more modern in this regard and international legal norms. Of course, it can not be said that the legal work for the purpose of ensuring international information security is completely absent, there are many useful initiatives reflected in some agreements, as well as within the framework of resolutions of the General Assembly of the United Nations. However, most of them are advisory and only focus on this issue. The leading countries of the world have not taken on any legally significant obligations in this area, therefore, there are no mechanisms of control and international legal responsibility.

Thus, both international and domestic law underestimate the risks associated with information technologies, do not take into account new information threats and do not provide the necessary regulatory influence on modern information relations.

This situation transforms the information sphere and information technology into attractive means of influencing state power and achieving its goals for any radical groups, not only hacktivists but also terrorists.

It is obvious that the times when it was possible within the framework of three articles of the Criminal Code of Ukraine to envisage, characterize and prohibit all crimes connected with information technologies have passed. The modern information sphere is far from the "sphere of computer information", which is already a fundamental dimension that permeates all aspects of the life of the individual, society and the state. Accordingly, qualitative and quantitative changes have also undergone threats existing in relation to it. Since the commissioning of the Criminal Code of Ukraine, many years have passed, during this time several information and technological revolutions have taken place, thousands of times the possibilities of consumer electronics have increased, new types of devices have emerged, the electronic market of goods and services has evolved, the form of information conflicts has changed, the influence of information technologies has intensified .

In this plan, the sources of military law describing threats related to the information sphere, information technologies and processes are useful. Their further development is capable of revealing the full potential of legal protection of the elements of information and cybernetic spheres. Taking as a basis the description of information and cybernetic threats, it is necessary to develop and consolidate, within the framework of the legislation on legal liability, new offenses, which accurately reflect the specifics of encroachments on the systems of the state, including military, management and critical objects, which provide for appropriate penalties.

The world's information sphere should be protected not only from crime but also from militarization, generally accepted principles and norms of international law, in particular the rules of law of armed conflicts and international security law, should take into account the military potential of information technology and regulate the order of activity of the respective forces and means for the purpose providing international information security. At the same time, the inviolability of civilian objects of informatization and the infrastructure of critical and dangerous objects of energy, transport, communications and industry should be ensured by mutual obligations of the states and mechanisms of international legal responsibility.

1. Kochergin AN Information and spheres of its manifestation: monograph. - Golitsyno: GPI of the Federal Security Service of the Russian Federation, 2008. - 272 p.
2. Wiener N. Cybernetics, or management and communication in the animal and the car. - Moscow: Nauka, 1983. - 344 pp.
3. Shannon K. Works on Information Theory and Cybernetics. - Moscow: Publishing House of Foreign Literature, 1963. - 825 p.
4. Kosice P. Cybernetics. From the human brain to the artificial brain. - Moscow: Publishing House of Foreign Literature, 1958. - 122 p.
5. Glushkov VM Cybernetics Questions of theory and practice. - Moscow: Nauka, 1986. - 488 p.
6. International Information Security: Diplomacy of the World: Sb. materials in common. Ed. SA Coma M. 2009. - 264 p.
7. Soviet Encyclopedic Dictionary / Ch. Ed. AM Prokhorov 3rd ed. M .: Sov. Encyclopedia, 1985.
8. Fateev K.V. Military security of the Russian Federation and legal regimes for its provision (theoretical and legal research). - M .: Military University, 2004. - 240 p.
9. Encyclopedia of the XXI century. Russian Weapons and Technologies. Volume XIII Systems of control, communication and radio electron fight / in common. Ed. S. Ivanov M .: Weapons and Technologies, 2006. - 695 p.