УДК 351.86:316.774:34]=111

V. I. Kunchenko-Kharchenko, *D.Sc., professor*
e-mail: itib@chdtu.edu.ua
O. M. Panasko, *Ph.D., associate professor*
e-mail: lena.pa@ukr.net
Cherkasy State Technological University
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

INFORMATION SECURITY IN UKRAINE. CONTEXT OF NORMATIVE LEGAL SUPPLY

In view of the rapid information technologies development, intensive implementation of information and telecommunication systems in various spheres of state's activity, modern world trends in information society, there is a need to consider the concept and content of information security. Due to the fact that today a number of main threats to the state's information security are realized in cybernetic space, special attention should be paid to the notion of cybernetic security as an independent component of Ukraine's national security in relation to the sphere of information security and its legal security. In the article an analysis of the current state for regulatory of information security is made from the point of view of an integrated approach, such as general requirements to information security, requirements to the security of information infrastructure and security requirements of information technologies.

Key words: *information security, national security, information resources, legal regulation in the field of information security, threats to information security, national security strategy, cybernetic security, information and telecommunication systems.*

Introduction. The current stage of society development is characterized by the growing role of the information sphere, which is a set of information, information infrastructure, entities that are engaged in the formation, dissemination and use of information, and the system for regulation of social relations that arise in this. Information sphere is a system-forming factor for the society existence, which has a powerful influence on the various components of state security, including political, economic, defense and others. Modern information technologies provide new possibilities for processing, transmission and storage of information and increase the level of information resources access for users. Today there is an intensification of the processes for informatization of state agencies, in the banking sector, the growth of powerful commercial structures, their integration at the international level, the aggravation of the criminal situation and a number of other factors, which causes a rapid increase in information security interest.

Problem statement and literature analysis. Information security plays an important role in creating a well-developed and protected informational environment, it is a determining factor in the interests of any state, is an indispensable condition for the development of society and the state. The presence of a developed information infrastructure, the powerful introduction of modern information technologies and systems, brings to the new level the processes of management at different levels, in particular state level, level of institutions, enterprises and organizations, levels of information and telecommunication systems.

The context of information security is of great importance, due to the growing importance and social significance of information, increasing its impact on all spheres of public life, increasing the amount of information accumulated in databases of different purposes, the complication of technical means, the development of technologies and other factors. The analysis of the sources proves that domestic and foreign researchers pay great attention of the information security issues. In this area it should be noted the works of O. Sosnin, V. Lipkan, B. Kormich, V. Grubov,

V. Domarev, I. Binko, V. Muntiyan, G. Pocheptsov, A. Lytvynenko, V. Buryachok, V. Butuzov, V. Tolubko, O. Dovhan, V. Khoroshko, S. Tolyupa and others. Among recent studies on information security it is reasonable to name the works of V. Bogdanov, V. Gorbulin, S. Gusarev, G. Ivaschenko, V. Kartashov, M. Levyts'ka, V. Lopatin and others.

The purpose of the article is to carry out a review of legal and regulatory provision in the information security sphere from the state level to the level of information and telecommunication systems, and to segregate the concept of "cybernetic security" in the context of information security and review its legal regulation.

The main part of the study. The concept of information security is connected with scientific research, practical human activities, the formation of regulatory and legal support. With information security related such concepts as the information environment of the society, interests in the information sphere, objects and subjects of information security, threats, principles of information security, types of information security and others (fig. 1). It should be noted that today in the scientific literature, among the specialists working in this area, there is no single approach to the concept of "information security". According to researchers, it can be interpreted as a state, process or activity, on the other side – as a property, ability, function.

In order to cover a variety of views on the definition of information security, it is advisable to classify them according to the content of approaches to this concept. As a result, some of them are listed below.

In a broad sense, information security is the state of the information environment security of society, which ensures its formation, use and development in the interests of citizens, organizations and the state.

By focusing on the processes of preservation, processing and information transmission, the notion of information security will become more restrictive, which will accordingly affect the definition of the term as the state of information security and its infrastructure against accidental or deliberate acts of a natural or artificial nature that can to cause unacceptable damage to the subjects of information relations, in particular, owners and users of information and infrastructure.

In terms of the main information properties as a security object, the "model CIA" is often used, which includes three defining properties: confidentiality, integrity and availability. Then information security is the preservation of the confidentiality, integrity and availability of information. Other specified properties may also be taken into account, such as authenticity, traceability, integrity and reliability.

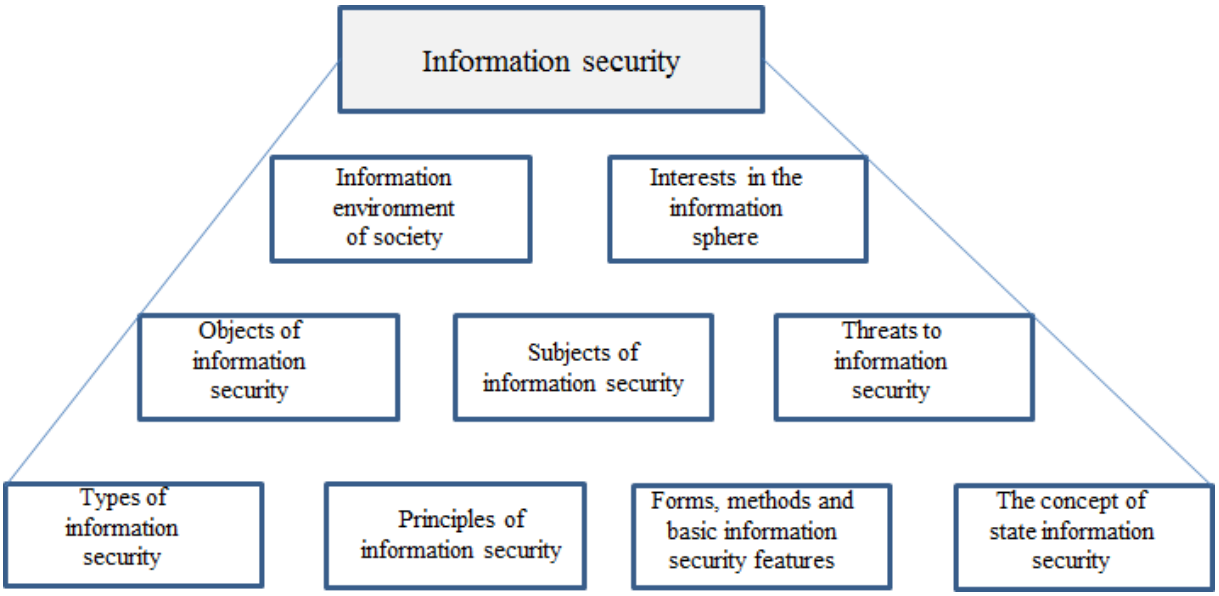

Fig. 1. Basic concepts related to information security

In the context of information law, the term "information security" is one of the aspects of the consideration for information relations in the information legislation sphere in terms of protecting the vital interests of the individual, society, state and focusing on the threats to the realization of relevant interests, and mechanisms for preventing or eliminating such threats through legal methods.

The concept of information security is closely linked to the protection of information sovereignty of the state, therefore, information security can be considered as the protection of internal information – the security of the information quality, its reliability, the security of various branches of information from divulgation, and the security of information resources.

Information security can be considered as a set of actions related to ensuring the right to information protection, the right to ownership of information, the right to protection against information and informational influences, and the right to information and freedom of information activity. In this regard, according to some researchers in the information security sphere, it is represented by three structural components:

– information and technical safety (information protection with restricted access in accordance with the legislation);

– information and psychological security (protection against informational influences that are negative);

– information security in the field of human and civil rights and freedoms (realization of the citizens right to information access, observance of the basic principles of information relations, in particular, the guarantee of the information right, openness, accessibility, reliability and completeness of information) [10].

The concept of information security is appropriate for its levels, in particular personality, society, state [9]. At the state level, the activities of state agencies in the aspect of information and analytical support, information provision of the interstate level in internal and foreign policy, the system of protection for information with restricted access etc. are presented. The society's level of information security correlates with the quality of the information and analytical space, the wide possibilities of obtaining information, the presence of independent powerful media. Information security of a person's level is characterized by the formation of rational, critical thinking, driven by the principles of choice freedom [1].

The analysis of the current normative base shows the inclusion of information security of Ukraine in the Ukrainian Constitution, in particular, in Article 17: "Protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important state's functions, the affair of the entire Ukrainian people", and in the complex normative legal acts of the Verkhovna Rada, the President of Ukraine, the Cabinet of Ministers, central executive agencies [2].

The Law of Ukraine "On the Concept of the National Program of Informatization" states that "information security is an integral part of the political, economic, defense and other components of national security", the objects of which are information resources, channels of information exchange and telecommunications, mechanisms ensuring the functioning of telecommunication systems and networks and other elements of the country's information infrastructure [5].

According to the Law of Ukraine "On the Fundamentals of National Security of Ukraine" as the main vector for ensuring the security of our state, information security is one of the public administration areas among such as: law enforcement, fighting corruption, border activities and defense, migration policy, education and science, scientific, technical and innovation policy, cultural development of the population and information security when a real or potential threats for national interests will appear [4]. Consequently, according to this law information security is a component of national security.

In the works of many scholars and researchers, information security is presented as an integral component and an independent direction of national security, in particular, B. A. Kormich characterizes information security as an information component of national security in the proportion of "part-whole" [10].

To date, a number of Ukrainian laws and other normative documents for different levels have been formed, which in general cover the problems of ensuring the state's information security, in particular, the laws of Ukraine ("On Information", "On Fundamentals of National Security", "On the State Service for Special Communications and Protection Information of Ukraine ", "On State Secrets", "On Protection of Information in Information and Telecommunication Systems", etc.), legal acts of the President

and the Cabinet of Ministers of Ukraine ("National Security Strategy", "Concept of information technical security in Ukraine"), international and state standards in terms of providing information security, normative documents of the information technical protection system, international agreements, the consent to which are allowed by the Verkhovna Rada of Ukraine, and substatutory legal acts issued for their implementation.

It should be noted that the Verkhovna Rada of Ukraine has not yet elaborated and not adopted some of the basic legal acts of this sphere, first of all, a law that would define the Concept of information security as a systematized set of data about the information state security and the ways of its provision, which provided the possibility to carry out system classification of destabilizing factors and information threats to the security of the individual, society and the state, the formation of the basic provisions of information state security ensuring and the development of proposals on ways and forms of information security ensuring.

According to information security which is characterized as an information component of national security and national security what is defined as state of safety from internal and external threats that ensures the existence of a person, society and state, which are guaranteed by the Constitution and Ukrainian laws, information security should be perceived as safety's state from external and internal threats in the information circulation sphere. Many researchers consider information security as a way that is opposed to internal and external threats.

In accordance with the Strategy of National Security of Ukraine [3], the main threats to information security were identified, in particular, information warfare against Ukraine, lack of integral communicative state policy, insufficient level of media culture of society, threats to cybersecurity and to information resources security caused by vulnerability of the critical infrastructure objects and state information resources to cyberattacks, physical and moral obsoleteness of state secrets protection and other types of information with the limited access; threats to the critical infrastructure security, caused by wear and tear of infrastructure assets and insufficient level of their physical protection, insufficient level of critical infrastructure protection from terrorist attacks and sabotage, and ineffective management of the critical infrastructure security.

Today there are new challenges the main threats to the state's information security, in particular, attacks on the state's information resources, the emergence of the conducting cyberwar concept, the creation of special structures in the armed forces of a number of world countries designed to conduction such a struggle, manipulation of public consciousness through the spread of inaccurate, incomplete or biased information, the appearance of threats to critical infrastructure objects of the state and society are unfolding in the cybernetic space. The new edition of National Security Strategy of Ukraine (№287 / 2015) [3], approved by the Decree of the President of Ukraine (May 26, 2005) for the first time distinguishes cybernetic security as an independent component of Ukrainian national security in relation to the information security sphere (Fig. 2). The penetration of information and telecommunication technologies in all spheres of public life causes the close connection of cybersecurity with other areas of national security, in particular, military, defense, economic, scientific and technical, ecological, etc. [8].

The main task of the state, economy and society both at the state and international levels is the issue of the cybernetic space defense. Much attention is paid to the legal regulation of cybernetic security issues. The main objective of the regulatory framework in the cybersecurity sphere is to create conditions and ensure the safe cyberspace functioning for the implementation of communications and social relations based on the unified communication systems, and the provision of electronic communications using the Internet and other global data transmission networks. In this direction the Strategy of Cybersecurity of Ukraine, the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" was developed [7].

The main subjects of the national cyber security system are the State Service for Special Communications and Information defense of Ukraine, the Security Service of Ukraine, the Ministry of Defense and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine, which carry out functions and tasks assigned to them in accordance with the Constitution and laws of Ukraine.

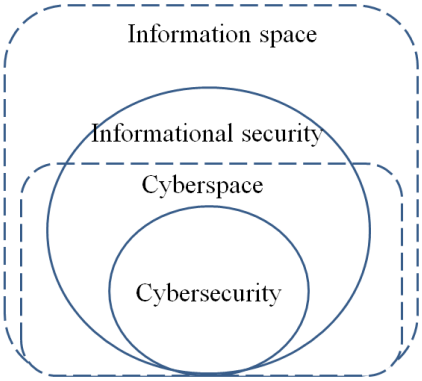

Fig. 2. Interconnection of information security and cybersecurity

The strategy defined priorities for providing cyber security and information resources, such as the development of state information infrastructure; creation of a cybersecurity system, development of the Computer Emergency Response Network (CERT); monitoring of cyberspace in order to detect, prevent and eliminate cyber threats in a timely manner; development of law-enforcement agencies' capacity to investigate cybercrime; security of critical infrastructure objects, state information resources from cyberattacks, refusal of software, in particular antivirus, developed in the Russian Federation; reforming the system of state secrets protection and other restricted information, state information resources defense, e-government systems, technical and cryptographic information security, creation of a cybersecurity training system for the security and defense sector; development of international cooperation in the cyber security sphere.

Information security is a problem of high complexity, which requires an integrated approach at different levels: state, institution or organization, level of information and telecommunication systems (ITS). At present, a significant amount of information resources focused on modern ITS are determined by commercial value, and that's why there is a tendency to increase the number of attacks and unauthorized access to information systems in order to capture the necessary information assets. The issue of information security in modern information and telecommunication systems and networks deserves due attention in the general aspect of information security. The basic regulatory documents for the design of protected information and telecommunication systems are the Law of Ukraine "On Information Security in ITS" [12] and a number of normative documents on technical protection of information. The standards of information security (international standards of ISO, domestic DSTU) have been developed to define requirements for quality indicators, control methods and evaluation of the information and telecommunication systems effectiveness. These normative documents define the bases and provisions of information security organization at all stages of the information and telecommunication systems life cycle. The using of information security standards for some organizations and institutions has a recommended character, while for others, in particular, for banking structures is mandatory.

At the level of institutions (organizations) management of information security is inextricably linked with the process approach. The International Standard ISO/IEC 27001 is based on the PDCA-model (Plan-Do-Check-Act), which structures and coordinates all processes of the Information Security Management System (ISMS). The sphere of ISMS includes the general organization, data classification, access systems, planning directions, employee responsibility, and the risk assessment using.

The list of standards in the ISO/IEC 27000 series includes about two dozen titles. These include, in particular, ISO/IEC 27000: 2005 (Definitions and Basic Principles), ISO/IEC 27001: 2005 (Information Security Management Systems), ISO/IEC 27002: 2005 (Practical Rules for Information Security Management), ISO/IEC 27003: 2010 (Information Security Management Implementation Guide), ISO/IEC 27005: 2011 (Information Security Risk Management), ISO/ IEC 27035: 2011 (Information Security Incident Management) and others. The introduction of standards for infor-

mation security management will reduce the estimated costs of developing, implementing and maintaining an information security system, managing risks, optimally identifying the most influential risks, minimizing their implementation, developing an appropriate and effective information security policy that will have a positive impact on the information security of institutions (organizations).

In general, it should be noted that the information security requirements are expedient at all levels of legislation, in particular, constitutional legislation, basic general laws, special laws, laws on the organization of the state system governance, departmental legal acts etc. The implementation of information security is carried out on the integrated approach basis and implemented at the state level, institutions and organizations and information and telecommunication systems, in compliance with the general requirements for information security, requirements for information infrastructure security and requirements for security of information technologies means.

Conclusions and prospects of research. The article defines the concept and content of information security, analyzes the status of regulatory and information security regulation as an integral part of Ukraine's national security, defines the legal regulation of the legal framework in the information security sphere, identifies the concept of "cybernetic security" and analyzes its legal basis. Particular attention is paid to the legal and regulatory framework for ensuring the information security of modern information and telecommunication systems.

References

1. Information security of Ukraine. URL: uk.wikipedia.org/wiki/information_bid_Ukraine
2. The Constitution of Ukraine (1996). URL: http://zakon4.rada.gov.ua/laws/show/254k/96-vr. Title from the screen.
3. Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the Strategy of National Security of Ukraine" dated May 26, 2015, No. 287/2015. URL: http://zakon2.rada.gov.ua/laws/show/287/2015
4. On the Fundamentals of National Security of Ukraine: Law of Ukraine dated June 19, 2003. URL: http://uadocs.exdat. com/docs/index-208817.html
5. About the Concept of the National Program of Informatization: Law of Ukraine dated 04.02.1998 No. 75.98-BP (1998). *Bulletin of the Verkhovna Rada of Ukraine*, No. 27–28, art. 182 [in Ukrainian].
6. About information: Law of Ukraine. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.
7. About the basic principles of providing cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII (2017). *Bulletin of the Verkhovna Rada of Ukraine*, No. 45, art. 440 [in Ukrainian].
8. Buryachok, V. L., Tolubko, V. B., Khoroshko, V. O., Tolyupa, S. V. (2015) Information and cybersecurity: sociotechnical aspect: textbook / ed. by Dr.Tech.Sc., professor V. B. Tolubko. Kyiv: DUT, 288 p. [in Ukrainian].
9. Bohush, V., Yudin, O. (2005) Information security of the state. Kyiv: MK-Press [in Ukrainian].
10. Oliynyk, O. V. (2012) Regulatory provision of information security in Ukraine. *Law and Society*, No. 3, p. 132 [in Ukrainian].
11. Kovtun, S. V. (2009) Information security: textbook. Kharkiv. KhNEU, 368 p. [in Ukrainian].
12. On the information protection in information and telecommunication systems: Law of Ukraine dated 04.19.2014. URL: http://zakon3.rada.gov.ua/laws/show/80/94-vr

Список літератури

1. Інформаційна безпека України. URL: uk.wikipedia.org/wiki/інформаційна_безпека_України
2. Конституція України, 1996. URL: http://zakon4.rada.gov.ua/laws/show/254к/96-вр. Назва з екрану.
3. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015. URL: http://zakon2.rada.gov.ua/laws/show/287/2015
4. Про основи національної безпеки України: Закон України від 19.06.2003 р. URL:

http://uadocs.exdat.com/docs/index-208817.html.
5. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75.98–ВР. *Відомості Верховної Ради України.* 1998. № 27–28. Ст. 182.
6. Про інформацію: Закон України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
7. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.
8. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.
9. Богуш В., Юдін О. Інформаційна безпека держави. Київ: МК-Прес, 2005.
10. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство.* 2012 № 3. С. 132.
11. Ковтун С. В. Інформаційна безпека: підручник. Харків: Вид-во ХНЕУ, 2009. 368 с.
12. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 19.04.2014 р. URL: http:// zakon3. rada.gov.ua/laws/show/80/94-вр

В. І. Кунченко-Харченко, *д.т.н., професор*
e-mail: itib@chdtu.edu.ua
О. М. Панаско, *к.т.н., доцент*
e-mail: lena.pa@ukr.net
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ. КОНТЕКСТ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Зважаючи на бурхливий розвиток інформаційних технологій, інтенсивне впровадження інформаційно-телекомунікаційних систем у різноманітні сфери діяльності держави, сучасні світові тенденції щодо інформатизації суспільства, з'являється необхідність у розгляді поняття та змісту інформаційної безпеки. У зв'язку з тим, що на сьогоднішній день ряд основних загроз інформаційній безпеці держави реалізуються у кібернетичному просторі, окрему увагу слід приділяти поняттю кібернетичної безпеки як самостійної складової національної безпеки України по відношенню до сфери інформаційної безпеки, а також його правовому забезпеченню. В статті проведено аналіз сучасного стану нормативно-правового забезпечення інформаційної безпеки з точки зору комплексного підходу, а саме: загальних вимог до інформаційної безпеки, вимог до безпеки інформаційної інфраструктури та вимог до безпеки засобів інформаційних технологій.

Ключові слова: *інформаційна безпека, національна безпека, інформаційні ресурси, нормативно-правове регулювання у сфері інформаційної безпеки, загрози інформаційній безпеці, стратегія національної безпеки, кібернетична безпека, інформаційно-телекомунікаційні системи.*