ON THE ISSUE OF INFORMATION SECURITY AS THE MAIN CONDITION FOR THE FORMATION OF A NEW INFORMATION SOCIETY: THE EXPERIENCE OF UKRAINE

Hisham Jadallah Mansour Shakhatreh[1]

[1]Ph.D. (Law), Assistant Professor, Faculty of Law, Jadara University, Jordan, e-mail: dr_hisham_shakhatreh@yahoo.com, ORCID: https://orcid.org/0000-0001-8693-5744

Citation:
Shakhatreh, H. (2022). On the issue of information security as the main condition for the formation of a new information society: the experience of Ukraine. *Economics, Finance and Management Review*, (2), 11–16. https://doi.org/10.36690/2674-5208-2022-2-11

Received: May 08, 2022
Approved: June 25 2022
Published: June 30, 2022

Abstract. *The concept of "information society" appeared in the process of scientific study of changes in society at the turn of the twentieth and twenty-first centuries. The basis of changes that affected almost all spheres of public life was the dominance of information and knowledge in the functioning and development of various spheres of social life (material production, employment and social structure, professional activities and lifestyle, culture, communication, etc.). The development of the global information society, wide use of information and communication technologies in all spheres of life has raised the problem of the information security. The main components of information security are a set of elements that include openness, confidentiality and integrity of information resources and supporting infrastructure. Studying the experience of foreign countries is necessary to create an optimal system of legal information security of Ukraine. Information security is a set of methods, techniques and actions aimed at protecting against unauthorized actions with data. Information is considered safe if it is fully protected from any kind of threat. The most common are cases of leakage of information about payments and personal data. The right approach to security is to take precautionary measures that can reduce harmful effects inside and outside the system. Information protection is a set of legal, technical, and organizational means of preventing unauthorized actions with data. It is installed in information systems and is characterized by a set of measures and actions aimed at protecting data from outside influences. Information security becomes especially important in the context of Ukraine's accession to global cybercivilization - the level of development of the information society, in which the efficiency of its components is determined by the achievements of scientific and technological progress: the development of computer information technology as a means of global telecommunications. Having studied the experience of foreign countries, we can offer some European methods for creating an optimal system of legal support for information security of Ukraine.*

Keywords: *information, information society, information security, information resources.*

JEL Classification: D80, F52, K39

Formulas: 0; fig.: 2; tabl.: 3; bibl.: 22

Introduction. In recent years information products and services have begun to play a key role in the economic sphere. In the political sphere, the availability of information related to state activities and political processes expands the possibilities for establishing effective feedback between the government and the population, which promotes the development of social initiatives and civil society. In the field of communications significant expansion of opportunities for communication and interaction in the range from interpersonal communication through chats, blogs, Internet forums, online conferences to interaction through so-called information networks within the global information space at the interstate and intercultural level.

Literature review. The term "information society" was proposed by the Japanese theorist K. Koyama. In Japan the program "Information Society Plan: National Goal to 2000", based on the work of a theorist was adopted back in 1972. However, the term "information society" was first used by Yu. Hayashi, a professor at the Tokyo Institute of Technology, in 1969. An important role in the approval and popularization of this concept was played by the work of another Japanese researcher I. Masuda "Information Society as a Post-Industrial Society", as well as books by Western futurists O. Toffler, J. Naisbitt and others. [1] Since the early 90's of the twentieth century, the term has entered wide scientific circulation.

Aims. The purpose of the article is to solve the problem of information security as a key area of development of the information society, and to determine the main directions of legal information security, taking into account the experience of the European Union.

Methods. The main research methods that were used in the article are general scientific methods of analysis and synthesis, as well as comparative analysis, which became the basis for obtaining research results.

Results. Information security is a set of methods, techniques and actions aimed at protecting against unauthorized actions with data. The Law of Ukraine "On Information" stipulates that information is any information and / or data that can be stored on physical media or displayed in electronic form [2]. Information is transmitted orally and in writing through signs, technical mechanisms, gestures, programs. Information and its constituent principles are still being studied by experts to improve the efficiency of data storage and use. The information that needs to be secured is used in various spheres of life: political, economic, social and spiritual. It is important to protect it from leakage to minimize possible adverse effects.

Information is considered safe if it is fully protected from any kind of threat. The most common are cases of leakage of information about payments and personal data (about 80% of cases). The right approach to security is to take precautionary measures that can reduce harmful effects inside and outside the system. *There is also a narrower meaning of information security:*

Information security is a practical activity aimed at preventing unauthorized access, use, detection and conversion of data. Internal and external information threats can harm national and international relations, specific citizens.

Information protection is a set of legal, technical, and organizational means of preventing unauthorized actions with data. It is installed in information systems and is characterized by a set of measures and actions aimed at protecting data from outside influences.

Information security is also the science of ensuring the preservation of information resources, inviolability of the will, legal rights of the individual and society. Penetration into the information space is an open (sometimes latent) action that specifically or coincidence affects the object of protection, leading to leakage or disclosure of information. Information security is based on the following issues:

1. Why, who and what to protect?
2. From what external and internal factors to protect?
3. How to protect against threats?

The main components of information security are a set of elements that include openness, confidentiality and integrity of information resources and supporting infrastructure. Security features often include protection against unauthorized access, which is a key component of data security.

Let us consider the system of basic components of information data:

- Accessibility is a feature that allows users in certain cases to freely obtain information that interests them. Exceptions are data hidden from public scrutiny, the disclosure of which can cause serious harm to subjects and information. For example, materials that everyone can receive are available: buying tickets, services at banks, paying utility bills.
- Integrity is one of the elements of information that guarantees its stability in case of intentional (unintentional) transformation or destruction of certain data. It can be static (stability of the main objects from the initial state) and dynamic (accurate implementation of successive actions). If the unity of information is violated, it can lead to serious negative consequences. This characteristic is the main and relevant in the information space.
- Confidentiality - the main property that allows access to information only to legal entities: customers, platforms (programs), processes. Confidentiality is the most researched and developed aspect of information security.

The purpose of confidential information is to restrict access of persons to data whose legal regime is established by specialized regulations in national and non-state industries, industry and social activities.

Information security becomes especially important in the context of Ukraine's accession to global cybercivilization - the level of information society, in which the effectiveness of its components is determined by scientific and technological progress: the development of computer information technology as a means of global telecommunications [3]. Against the background of the formation of the global information society and Ukraine's entry into the world information space, increasing the effectiveness of legal regulation of information security is becoming especially important. Moreover, a person, his or her life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value [4]. The most important feature of the information society is the ability of everyone to create information and knowledge, have access to them, use and share them. The main goal of the information society is to enable people to realize their intellectual potential, their capabilities and abilities, contributing to the constant development and improvement of their living standards. In the practice of information society in different countries there are three main models: European, American and Asian.

The European model of information society development is characterized by social orientation and active involvement of the state and international institutions. EU bodies are implementing a number of programs of the information society development and a single European information space creation. These programs are aimed at ensuring the rights and freedoms of citizens, the development of information infrastructure, free access and awareness of society, the creation of favorable conditions for the development of entrepreneurship in the field of information technology. A sign of the European model of information society is the variability of political orientation of programs for building and developing the national components of Europe, due to the new regional geopolitics, information (intellectual) economy, information legislation, various opportunities for post-industrial development [1].

Ukraine does not stand aside from the process of forming an information society. One of the main priorities is the desire to build a people-oriented, open and development-oriented information society in which everyone could create and accumulate knowledge and information, have free access to them, share, use, thus promoting social and personal development and improving the quality of life. Moreover, Ukraine has formed the legal basis for building an information society: laws of Ukraine "On the Concept of the National Informatization Program" and "On the National Informatization Program" were adopted, as well as other regulations governing public relations for the creation of electronic information resources, protection of intellectual property resources, introduction of electronic document management, information protection. These and other preconditions allow us to believe that the Ukrainian market of information and communication technologies is in a state of active development and can become the foundation for the development of information technology information society in Ukraine.

Due to the active development of our country and its active cooperation with the European Union Ukraine is increasingly trying to bring all areas of activity to European norms and standards. In addition, the pace of digital development is increasing. That is why there is a need for a comprehensive study of the experience of international legal information security, its systematization, the formation of strategies for further improvement of the national information security system, taking into account the development trends of Ukraine. Despite the fact that the issue of information security attracts considerable attention of researchers and scientists, there is still no single and systematic scientific study of improving the administrative and legal support of information security in Ukraine, taking into account the experience of foreign countries, especially Europe.

The study of the experience of foreign countries in the field of information security began in 1991, when European countries (at that time, not yet the European Union) developed the first standard of information security "European criteria for information security". This document defines the tasks of information security, especially the protection of information resources from unauthorized modification or destruction, to ensure the confidentiality and integrity of information resources, as well as ensuring the efficiency of all systems by combating threats of denial of service. In 1996, after the creation of the European Union, information security standards were officially published in the document "Common conditions for information technology security". According to it, the CIA TRIAD model was used to describe the main criteria of information security. The main characteristics of information security of this model are:

- confidentiality;
- integrity;
- availability.

Later, in 2001, the European Commission presented a document entitled "Network and Information Security: A European Policy Approach", which set out the

European Union's current approach to information security issues. This document identified the main directions of European policy in the field of information security, namely raising awareness of all users about the possibility of a threat when working with communication networks; creation of a single European information and warning system for new threats; providing comprehensive technological support; support and promotion of market-oriented standardization and certification; legal support, the priorities of which are the protection of personal data, combating cybercrime; strengthening information security in general at the state level by introducing effective and uniform means of information security and encouraging the use of electronic signatures in the provision of public online services of member countries, etc.; development of international cooperation in the field of information security.

European standards of information activity of public authorities provide for their total information openness, except for restrictions related to the confidentiality of information (primarily, ensuring the security of personal data). Directive 95/46 / EC "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" is the main document regulating the right of citizens of the European Union to the protection of personal data [5]. It is important to note one of the provisions, namely the "Guaranteed Security Principle № 11", which requires that personal data be protected by reasonable means of security against all types of threats, such as data loss, unauthorized access, destruction, use, modification or disclosure. The new rules on personal data protection were approved on April 14, 2014 and came into force in 2018. An innovation was the introduction of more severe penalties for late reporting of information leaks. This directive requires the consent of users to the processing of their personal data, which must be free, informed and specific, and can be revoked at any time.

Discussion. Having analyzed these provisions, it should be noted that the development of legal regulation and harmonization of relevant standards for information security, including information technology security, in the European Union began to develop much earlier than in Ukraine, so it is more systematic and thorough. In addition, the regulation of information security in the European Union is clearer and more structured. First of all, these are clearly defined basic concepts and categories, the implementation of a list of relevant threats to information security, such as personal data, etc.

On the example of assessing the system in Germany and Poland, we can conclude that to achieve the goal of information security in any sphere of public life requires a clear and coordinated functioning of the subject of such security, which is endowed exclusively specialized powers. It is the specialized body that can most effectively ensure information security, as it accumulates special experience, improves educational, technical, material, practical base, as well as the baggage of interaction with other subjects of legal relations in the state and subjects of international law. On the example of Germany, it is clear that the appropriate basis for the further effective functioning of the legal mechanism for information security in the country is, first of all, effective and high-quality regulatory regulation [6, 7].

One of the most important trends to be borrowed in Poland in the context of information security is the active involvement of non-state actors in all processes, especially members of civil society. After analyzing such implementation in other countries, it is necessary to note the positive impact on the whole sphere, as well as that information security is carried out primarily by adopting a key strategic document that directs the activities of all actors in information security, identifies key areas and tasks set before the mechanism of information security. Thus, having studied the experience of foreign countries, we can offer some European methods for creating an optimal system of legal support for information security of Ukraine.

Conclusion. The main components of information security are a set of elements that include openness, confidentiality and integrity of information resources and supporting infrastructure. Studying the experience of foreign countries is necessary to create an optimal system of legal information security of Ukraine. Information security is a set of methods, techniques and actions aimed at protecting against unauthorized actions with data. Information is considered safe if it is fully protected from any kind of threat. The most common are cases of leakage of information about payments and personal data. The right approach to security is to take precautionary measures that can reduce harmful effects inside and outside the system. Information protection is a set of legal, technical, and organizational means of preventing unauthorized actions with data. It is installed in information systems and is characterized by a set of measures and actions aimed at protecting data from outside influences. Information security becomes especially important in the context of Ukraine's accession to global cybercivilization - the level of development of the information society, in which the efficiency of its components is determined by the achievements of scientific and technological progress: the development of computer information technology as a means of global telecommunications. Having studied the experience of foreign countries, we can offer some European methods for creating an optimal system of legal support for information security of Ukraine.

References:

1. Tsymbaliuk V. S. Informatsiine pravo (osnovy teorii i praktyky) [Information law (basics of theory and practice)] : monohrafiia. Kyiv, 2010.
2. Zakon Ukrainy «Pro informatsiiu» ["On information"] // Vidomosti Verkhovnoi Rady (VVR). 1992. No 48. St. 650.
3. Tsymbaliuk V. S. Sutnist informatsiinoi bezpeky v umovakh vkhodzhennia Ukrainy do hlobalnoi kibertsyvilizatsii [The essence of information security in the context of Ukraine's entry into global cybercivilization] // Naukovyi visnyk akademii DPS Ukrainy. 2007. No 4. P. 174 –178.
4. Konstytutsiia Ukrainy [Constitution of Ukraine] // Vidomosti Verkhovnoi Rady (VVR). 1996. No 30. St. 141.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal L 281. 23/11/1995. - P. 0031-0050.
6. Tkachuk T.Y. Zabezpechennia informatsiinoi bezpeky u krainakh tsentralnoi Yevropy. [Ensuring information security in Central Europe.] Yurydychnyi naukovyi elektronnyi zhurnal. 2017. № 5. URL: http://lsej.org.ua/5_2017/30.pdf
7. Salaev T.H. Opyt zarubezhnykh stran v kontekste usovershenstvovanyia adminystrativno-pravovogo obespechenyia informatsyonnoi bezopasnosty v Ukrayne. [The experience of foreign countries in the context of improving the administrative and legal support of information security in Ukraine.] Chasopys Kyivskoho universytetu prava. 2020. №5. P. 403-407.