INFORMATION SECURITY AS AN OBJECT OF REGULATION IN THE LAW OF UKRAINE

Iryna M. Sopilko
Doctor of Law, Professor; National Aviation University
1 Liubomyr Huzar Ave., Kyiv, Ukraine, 03058
https://orcid.org/0000-0002-9594-9280
iryna.sopilko@npp.nau.edu.ua

ABSTRACT. The study gives definitions of information security and related terms, such as cybersecurity, national security, and others, indicates the goals, objects, subjects of the concepts under consideration. The author also considers the features of the foundation and development of the information society in Ukraine, the components of its state information policy for ensuring information security, and identifies the key operations of activity of state bodies in the information sphere. The approaches of scientists who studied certain aspects of national and information security were analyzed, based on their work valuable conclusions were drawn and the conceptual basis of the article was formed. Independently, the definition and characteristics of external and internal threats to the information security of the country are given, methods for solving the problems arising in this connection are introduced, ways of ensuring the information security of the state are indicated.

Information security in this study is considered as the central element of the national security of Ukraine, as well as a problematic issue in the field of information protection and ensuring the high-quality functioning of the information space. The author made an in-depth analysis of the existing regulatory and legal instruments for ensuring information security, pointed out their shortcomings, and gave recommendations for their further advancement. Also, recommendations are given to improve the current situation with the regulation of information security in the country, the directions of the state information policy are suggested and ways to ensure the continuity of the functioning of the information security system of Ukraine are indicated.

Keywords: information security, InfoSec, information society, information, cybersecurity, cyberspace.

INTRODUCTION

Today, Ukrainians can observe the rapid growth of digitalization: we own property in the form of digital assets, exchange digital data, order, and provide digital services. Back in 2007, the Law of Ukraine On the Basic Principles for the Development of an Information-Oriented
Society in Ukraine for 2007–2015 as one of the main priorities of our state of Ukraine indicated the desire to make our society truly informational, open to everyone, oriented for human interests. With this act, our authorities wanted to create a society in which information and knowledge would be available to everyone, and everyone could create and use, exchange such intangible assets, which would contribute to the social development of the Ukrainian people and improve the quality of their life (“On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015: Law of Ukraine of January 9, 2007 № 537-V,” 2007).

Indeed, today it is information that is not just a highly valuable resource, but also a way of influencing individuals, groups, and even governments of countries. Therefore, the virtual space is not considered completely safe; terrorist and other criminally punishable acts are often committed in it.

Taking into account the current state of affairs in the world regarding the protection of the cyber information space, Ukraine strives by all available means to improve the level of information security as the basis for the security of the state as a whole.

It is information security that will protect the information society in particular and the state of Ukraine as a whole. And this is what allows our society to achieve its goals in the field under discussion. That is why this paper will be devoted to the problem of information security, its essence, potential risks, correlation with cybersecurity and probable ways of solving the emerging problems and threats in this field.

For Ukraine, the topic of information security as the basis of state security and its legal regulation is relatively new and still little developed. There are not so many comprehensive studies on this issue, but there are considerations of certain categories and issues of information security. T.S. Perun (2019) analyzed the administrative and legal mechanism for ensuring information security in Ukraine and provided his scientific approach to determining its essence. According to it, in the context of the development of the information society and aggression in the eastern part of Ukraine, information security is a special state of security of information resources, information technologies, and databases as well as technical means that are required for processing and collecting, storing and communicating information. In this context, such information is used to implement the rights, freedoms, interests of the individual, society, and the state as subjects of information activities in the information space. A. Yu. Nashinet-Naumova (2017) in her monograph highlighted the issues of legal regulation of information security. O. O. Zolotar (2018) considered the theoretical and practical foundations of the functioning of human information security. Ensuring this type of security as a function of a modern state is considered in the monograph by O. O. Tikhomirov (2018). The practical problems of introducing new information security standards in the context of the development of the national cybersecurity system were studied and highlighted by S.L. Gnatyuk (2018).

The features of the formation and development of the information society in Ukraine are disclosed in more detail. D.V. Dubov, M.A. Ozhevan, S.L. Gnatyuk (2010) revealed the modern understanding and concept of the information society, developed recommendations and forecasts for the subsequent implementation of information technologies in Ukraine and the world. L.V. Lopa and V.A. Koziryev (2017) made a detailed analysis of the characteristics
of the information society, discussed its negative and positive aspects, investigated the existing programs for the formation of such a society both in Ukraine and in the world. T.V. Pisarenko, T.K. Kvasha and others (2015) studied the experience of Ukraine in building an information structure to ensure the innovative development of our society and provided proposals for creating a system of information and analytical support for state innovation policy in Ukrainian country. O. A. Zayarny (2018) described in detail the administrative and tort aspects of the legal support for the development of the information sphere of the State.


Therefore, we can safely say that the state information policy is an important element of the country's foreign and domestic policy, covering all spheres of the life of Ukrainian society. It is precisely the provision of a sufficient level of information security in the state that is the main prerequisite for ensuring a solid and reliable basis for the functioning of national security in the country. With this research, the author wants not only to explain the significance and role of information security for modern Ukraine but also to develop recommendations for maintaining it at the proper level, to give a special analysis of the legal resources for regulating this issue. This is especially important in connection with the rapid development of the information sphere, which is accompanied by the emergence of radically new threats to the interests of every Ukrainian citizen, Ukrainian society, the Ukrainian state, and its national security.

OBJECT AND SUBJECT MATTER OF THE STUDY

The object of the study is social relations regulated by administrative, civil, and criminal law, arising in connection with ensuring information security and implementation of the rights of subjects of information activities. The subject matter of the study is information security as the basis of Ukraine’s national security.

PURPOSE OF THE STUDY

The purpose of the study is to determine the legal nature of information security as the basis of Ukraine’s national security, to identify deficiencies in the approaches of its legal regulation, and to formulate suggestions aimed at improving legislation to protect and maintain information security as the basis of Ukraine’s national security at a proper level.

Almost instantaneously we figure out the author's intentions, their agenda, and our relationship with him.
MATERIALS AND METHODS

The methodological basis of the study is represented by the universally recognized scientific objectivity criteria and several general scientific cognition methods that provide a comprehensive analysis of information security as the basis of Ukraine's national security. The application of the systematic method helped to establish the link between information security and national security and cybersecurity, as well as other related phenomena; and helped to determine the place of information legal relations in the Ukrainian legal system. The author of the study also used such methods as formal-logical (it helped to analyze in detail and deepen the conceptual apparatus); historical (made it possible to periodize the sources of normative regulation of the legal relations in question); method of classification and grouping (to determine the object-subject composition in disputes regarding state information security).

A comparative legal method was also used, which made it possible to clarify the problematic issues of law enforcement in the information security field and to compare the procedure and conditions of implementation of the techniques and means to ensure the maintenance of information security at the proper level. The methods of analysis and synthesis, together with the synergistic method, provided the basis for a comprehensive study of the problematic aspects of the process of acquiring and exercising the rights to obtain and dispose of information resources by a person, society, and the state. The modeling method provided the development of suggestions for improving legislation in the field of regulation of issues of ensuring the necessary level of information security in Ukraine.

The author analyzed in detail the regulatory legal acts of Ukraine as well as relevant international directives and acts on information security, national security and cybersecurity, studied the practice of applying legislative acts, reviewed the judicial investigative practice on this issue.

RESULTS AND DISCUSSION

The widespread development of information technology tools and technological progress has made it possible for us to easily receive, store, process, and transfer information in huge volumes and at a very fast speed, which previously seemed simply impossible. The modern stage of informatization of Ukrainian society and the state as a whole is associated, in particular, with the use of computer and telecommunication systems. Accordingly, today there is a significant increase in the need for the development and application of effective practices and solutions in the information field, especially in the field of information security (also known as InfoSec). For a better understanding of the essence of the issue and the search for solutions for it, we consider it necessary to first define the basic conceptual categories and constructions considered in this research.

As already mentioned, our Ukrainian society aims to become informational. However, it is important to understand what the information society is. There are many ways to define this term, including the following:
• it is a human-centered society, it is open to everyone, its main goal is to contribute to development. In it, each individual can create information and knowledge, have access to them, freely apply and exchange such data. Consequently, it will allow individuals, groups, and even entire peoples to fully realize their potential and progress, improving the quality of their lives (World Summit on the Information Society (Geneva 2003 – Tunisia 2005), 2006);

• it is a society in which everyone, anywhere, at any time, can obtain any information and knowledge both free of charge and for a fee through automated access and communication systems. At the same time, the indicated data are important for the life of people and the solution of certain problems (Zgurovsky, 2006);

• it is a society in which information technology is the basis for economic development, and which is socially transformed to help people and social groups to use ideas and knowledge, as well as which favors people to empower their potential (“MOFA: Okinawa Charter on Global Information Societ,” 2000);

• it is a society that was formed as a result of the new industrial revolution. This happens based on information and telecommunication technologies and based on information as an expression of human knowledge. It is the technological progress that contributes to the fact that the processing, collection, receipt, and exchange of data in any form were not limited due to time, distance, or size (“Europe and the Global Information Society. Recommendations to the European Council,” 2000).

The Ukrainian government, in the previously mentioned Information-Oriented Society Development Law (Verkhovna Rada of Ukraine, 2007), has identified the following main strategically important goals for the development of the information society in the country:

• ensuring computer and information literacy of the Ukrainian people through the development and institution of an appropriate education system;

• creation of information systems of the state, especially in the field of health care, science, and education, and the like;

• the fastest development and implementation of innovative competitive information and computer technologies, first of all, in the public administration system;

• development of the Ukrainian information infrastructure with the possibility of its subsequent integration with the global infrastructure;

• provision of state support to the “electronic” sector of the economy;

• protection of information rights of Ukrainians and minimization of the risk of “information inequality”;

• improvement of legislation on information relations;

• improving the situation of information security through the use of innovative technologies, and so on.

The formation of the information society is ensured with the help of the latest information and telecommunication technologies, which open up completely new opportunities for international information exchange for us. The very same formation of the information society forms the global information space, which is inextricably linked with cyberspace. Let’s study these concepts. According to V.N. Yasenev, the information space (also – the infosphere) is a sphere of human activity, which is directly related to the production of
information, its consumption, and modification, it includes, among other things, information resources, information itself, and its flows (Yasenev, 2017). And cyberspace, according to the Oxford Lexico Dictionary, is a conditional environment in which subjects communicate with the help of computer networks (Oxford University Press (OUP), 2020). Also, according to Denise M. Carter, cyberspace as a measure of social activity and the life of people is a new, globally accepted locale for conducting everyday social activities and the main concept in the study of cyberculture (Carter, 2020).

Having defined the concept and goals of the information society, cyberspace and the like, we will proceed to study directly information security and related national security and cybersecurity. The concept of information security can be viewed from several angles. Thus, according to V. S. Tsimbalyuk and A. V. Babinskaya, the InfoSec of our country is a state of protection of national interests in the information environment, which is determined by a complex of balanced interests of the individual, society, and the state itself (Tsymbalyuk & Babinska, 2014).

A.A. Nishchimenko has an almost identical definition, to which is added an indication of protecting the interests of the above subjects from internal and external threats. Also, to the state of security, scientists put forward a requirement for compliance with the principle of ensuring national security in the information sphere (Nishchimenko, 2016). L.A. Kochubei has a slightly different understanding of information security: this is a special state of protection of vital interests and with them the information security of information subjects, in which any informational influences on them do not cause destructive thoughts or actions, the result of which will be negative deviations in the development of these subjects (Kochubey, 2015).

Information law specialist I. V. Panova defines information security as one of the elements of considering information legal relations within the framework of information legislation from the point of view of protecting the essential interests of information subjects. At the same time, she focuses on countering the threats of the indicated interests and on the mechanisms for eliminating such threats through legal instruments (Panova, 2018).

Accordingly, the author of this study suggests understanding information security as a certain state of security of the information environment of the Ukrainian society, because of which such a society as an information subject (including individuals, groups, the state as a whole) can freely develop informationally and be sure that its information interests and rights will be protected from internal and external threats.

It can be emphasized once again, according to the studied scientific works, that the subjects of information security are directly Ukraine as a state (it carries out its functions in this area through the relevant bodies), each of us as a separately taken citizen, groups and associations, which are prescribed by law with special functions of ensuring information security. Furthermore, the author of this study believes that the object of Infosec should be considered the human psyche, his consciousness, as well as the consciousness of the masses, as well as information systems for various purposes. If we consider the issue of defining an object from a sociological point of view, then an individual, a collective, a society, a state, and the world community will be considered as such.
The purpose of InfoSec is considered to be the security information support of the activities of information subjects. In this regard, the following four levels of formation of the Ukrainian information security regime can be distinguished:

1. legislative (includes regulations such as laws, standards, and the like);
2. administrative (involves measures and means to protect InfoSec, determined by the management of the organization);
3. procedural (assumes security measures associated with specific people),
4. program-technological (assumes specific technical measures) (Mocherny, 2000).

The high-quality creation of a system for ensuring information security in Ukraine has a certain complexity and therefore requires the development of theoretical and methodological foundations and a legal mechanism for the implementation of innovative reforms. As the main regulatory direction, the author of this study chose the administrative-legal mechanism for ensuring information security, since it is it that especially strongly influences the effectiveness of the implementation of administrative and legal methods and tools in the area under consideration. And it is it which, as a result, provides a sufficient level of protection for the interests of a person, society, and the state as a whole. However, criminal law, civil law and not only are also used concerning information security relationships.

The main regulatory documents on the regulation of information security of Ukraine are the Constitution, the Decree of the President of Ukraine On the Decision of the National Security and Defense Council “On the Doctrine of Information Security of Ukraine”, the resolution of the Verkhovna Rada of Ukraine on the main directions of the foreign policy of our country and the following laws:

- “On the National Security of Ukraine” and “On the Concept of the National Informatization Program” – they are devoted to the specifics of ensuring national information security and related matters;
- “On the basic principles of ensuring the cybersecurity of Ukraine” represents the features and objectives of ensuring the protection of the rights of subjects in cyberspace;
- “On information” defines information, contains rules on its application, also together with the Law “On the Concept of the National Informatization Program” fixes the tasks and directions of Ukraine’s activities in the information environment determines the features of its development,
- “On state statistics”, “On information protection in automated systems”, “On scientific and technical information”, “On access to public information”, “On the national archival fund and archival institutions”, “On state secrets”, “On telecommunications”, “On Television and Radio Broadcasting”, “On Print Media ” contain provisions on the procedure for the cooperation of authorities with the subjects of information and information-infrastructure relations, on the types of information, its use, on the procedures of state regulation in this area,

But, before proceeding to the analysis of the legal instruments for ensuring InfoSec, it is worth giving a definition to such a concept as national security. According to Article 1
(clause 9) of the Law on National Security, this will be considered protection from real and potential threats to state supremacy, territorial integrity, democratic constitutional order, as well as other national interests of the state. Also, the author of the study would like to note article 31 of the said Law, dedicated to the document of long-term planning – the Ukrainian cybersecurity strategy. This act defines the main goals of the national interests of the state in the field of cybersecurity, indicates the probable and already existing cyber threats to the vital interests of our society, nation, the state in cyberspace. The Strategy also indicates the main approaches and directions in the implementation of state policy regarding the safe existence of cyberspace, which should be used in the interests of the three subjects of information security. The considered norm also mentions increasing the effectiveness of the main subjects of ensuring cybersecurity among the goals of the Strategy ("On the national security of Ukraine: Law of June 21, 2018 № 2469-VIII," 2018).

In connection with the above, it is worth defining cybersecurity. Following Article 1 (Clause 5) of the Law of Ukraine On the Basic Principles of Cybersecurity, this is recognized as the security of the vital interests of a person, society, and country when using cyberspace. And in the presence of such security, the sustainable advancement of the information society and the digital communication environment will be sufficiently ensured, and probable and real threats to the national security of the Ukrainian state in cyberspace will be detected, destroyed, or prevented promptly ("On the basic principles of cybersecurity in Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII," 2017).

It is also important not to confuse the concepts of cybersecurity and information security, as many often perceive them as synonyms. As Yu. Gudz points out, cybersecurity is the security of IT systems, namely hardware and software. At the same time, information security is the security of information in information systems, for example, of a certain enterprise. Cybersecurity is an element of an organization’s information security. He also gives a vivid example of this. So, the issue of cybersecurity is how secure your laptop is. And already under the jurisdiction of InfoSec is whether you attach a piece of paper with a password to your profile on the social network on your laptop (Gudz, 2017). The author of this study wants to give her example in this regard: it is enough to imagine an umbrella. In this case, the umbrella’s dome is information security, and the things that this dome protects against “rain” (threats) are cybersecurity and other elements of the InfoSec, for example, cryptography.

The author of the work also wants to draw attention to Part 1 of Art. 17 of the Ukrainian Constitution, taking into account that InfoSEc is a vital element of national security. This norm directly prescribes that ensuring the economic and information security of our state is just as important a function for the authorities and all Ukrainians as ensuring sovereignty and territorial integrity ("Constitution of Ukraine: Law of 28.06.1996 № 254k / 96-BP," 1996).

To understand what InfoSec is guarding and what it fears, it is important to know the main threats to it. Note that in this case, everything is considered a threat that can use a vulnerability to breach information security, as well as malicious changes, deletion, or corruption to information resources. Therefore, the threats can be divided according to the purpose of the method of influence:
• methods used by hackers to exploit vulnerabilities in the components of the victim's system;
• the impact of threats on the victim's assets.

Also, which is considered more reasonable by the author of the study, Infosec threats can be divided into external and internal, and each group of threats, according to M. Jouini, can be admitted in connection with human activity (malicious, nonmalicious), environmental vulnerability (nonmalicious) or technological vulnerability (nonmalicious) done accidentally or intentionally. These are such threats:
• destruction of data,
• theft and loss,
• denial of use or illegal use,
• damage,
• disclosure,
• elevation of privilege (Jouini, Rabai, & Aissa, 2014).

The previously named information subjects often face negative influence from these threats. Quite often, as V.M. Furashev points out, victims are confronted with a situation when in the state of location of the source of information, such information is completely legal and authorized, and in the state of the victim, it is unauthorized under local legislation. Accordingly, the use of modern information technologies affects the level of information security of information subjects (Furashev, 2012).

As mentioned earlier, the essential components of information security are the so-called CIA triad: availability (that is, the ability to receive the necessary or related service within a certain time), integrity (information must be reliably defended from illegal modification, disruption, must be relevant and consistent), confidentiality (information must be shielded from unauthorized access). In connection with the above, the author of the article considers it necessary to pay attention to the issue of violation of the integrity and availability of information, its confidentiality. Article 20 of the Law of Ukraine On Amendments to the Law of Ukraine On Information divides information according to the order of access into open and information with limited access. The essence of the latter is described in article 21 – it is confidential, secret, and proprietary information (“On Amendments of the Law of Ukraine ‘On information’: Law of Ukraine of 13.01.2011 № 2938-VI,” 2011). The same provision is contained in the Law of Ukraine “On Information”, except for the phrase “official information (“On information: Law of Ukraine of October 2, 1992 № 2657-XII,” 1992). If we turn to the definition given in Articles 7-9 of the Law of Ukraine On Access to Public Information, we can conclude that not only violation of confidentiality of information harms and negatively affects the individual and the Ukrainian society, but also a violation of the regime of access to information, which is established by national legislation (“On access to public information: Law of Ukraine of 13.01.2011 № 2939-VI,” 2011).

In conclusion, it can be argued that the organization of legal regulation of information security in Ukraine is carried out based on clearly defined principles that are the foundation for the functioning of the country’s information security system. Therefore, in the administrative and legal regulation of the specified security, it is important to take into account the following:
• information security regulation standards should be uniform and obligatory for all subjects, which will make it possible to predict the future effect of information activities;
• for violation of the rules, strict and inevitable punishment should be provided;
• ensuring information security should concern all actors in the information sphere and consumers of information services;
• it is necessary to form legal consciousness in participants in information activities, to teach them law-abiding behavior.
With this approach to legal norms and regulation of InfoSec issues, Ukraine will be able to achieve a balance of economic interests and would be respected as a country with an information society.

CONCLUSIONS

Analysis of the means and peculiarities of the legal regulation of information security as the basis for the functioning and stability of the national security of Ukraine gave the author of the study the opportunity to draw certain conclusions and make recommendations on the issues considered. First, during the research, the author’s definition of information security was provided: it is a certain state of security of the information environment of the Ukrainian society, because of which such a society as an information subject (including individuals, groups, the state as a whole) can freely develop informationally and be sure that its information interests and rights will be protected from internal and external threats. It follows from the above that the object of protection is the information itself, its creation, use, security and the subjects are those who perform these actions (people, society, the state represented by the responsible authorities). However, there is no information for information’s sake. All knowledge and data exist as long as they are needed. And it is the information subjects that determine this need.

Secondly, the author concludes that harm is caused due to imperfect regulation of information relations, as well as due to the use of low-quality information, and the like is the evidence of the decline in information security in the country. Accordingly, the following problems of ensuring information security in our country are still seen as unsolved:
• there is an imperfection of both the information policy in general and the information security policy itself;
• there is a considerable number of gaps in the regulatory framework that deals with these issues, it requires improvement and harmonization with the current international standards;
• the activity of officials, various formations, and groups in the information sphere is insufficiently regulated and sometimes does not comply with the requirements of the legislation;
• the information infrastructure of Ukraine should be reformed to better ensure the rights and freedoms of information subjects.

According to the results of the study, several additional questions arose: how to ensure an appropriate level of information security in the country, how to effectively assure the integrity of information in all spheres of the life of the Ukrainian society, what means can
be used to prevent deliberate falsification of data, and some others. The answer to these questions lies in the choice of ways to solve the problems of ensuring information security of Ukraine at the proper level. It consists of a combination of constituent and regulatory and administrative-organizational acts with the means that allow countering threats and challenges in the field of information security.

Hence, the state information policy should reflect the pressing issues that have developed in the international sphere and directly in the field of information security. It is necessary to recognize and implement the provision of the regulatory and legal protection of the rights and interests of all subjects of information relations, namely individuals, social groups, society, and the state in general.

The following should become the basis for the directions of the state information policy:

• ensuring the subjective right to reliable, comprehensive, and timely information;
• assuring the development and use of the information environment in the interests of people;
• guaranteeing the subjective right to freedom of speech and information activity;
• provision of state support to entities for the development of information technologies;
• ensuring an appropriate level of information culture of the individual, which, regardless of the presence of information threats, will allow him to realize his vital interests in the information society;
• providing information and national-cultural identification of our country in the global information space;
• limiting government interference in the internal organization of information processes, except for cases stipulated by law.

Harmonious provision of information security of the state, individual, and society is a complex process that involves efforts and special activities of the authorities in cooperation with leading organizations in the field of information and cybersecurity, individual stakeholders and directly practicing lawyers and representatives of the Academia field.

REFERENCES


