ISSUES OF DETERMINING THE CONTEXT OF RESTRICTED INFORMATION SECURITY

Dmytro Kots
Head of the Legal Sector of the Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
e-mail: dyadyakots@ukr.net, orcid.org/0000-0002-3955-7100

Maksym Kudrytskyi
Ph.D., Scientific Secretary of the Scientific Council's Secretariat, Central Research Institute of the Armed Forces of Ukraine, Ukraine
e-mail: kma_13@ukr.net, orcid.org/0000-0003-1554-4732

Valentyna Dolia
Scientific Researcher, Central Research Institute of the Armed Forces of Ukraine, Ukraine
e-mail: dolyav0401@gmail.com, orcid.org/0000-0003-1139-3519

Summary

The article analyzes the problematic issues of determining the content of the concept of protection of restricted information, in particular, the authors analyze the existing terminology used by the legislation of Ukraine on the protection of restricted information.

The authors of the article, based on existing legislation regulating such information storage measures as information protection, technical protection of information, cryptographic protection of information, cyber protection, using the deductive method of research derived the definition of "protection of restricted information".

In addition, using various scientific research methods, the authors of the article highlight the issues of legal uncertainty and contradictions in the concepts of some types of restricted information protection, which are found in the guidance documents on the subject of research.

Also, in the article:

the properties of information are derived and the types of operations with information are determined. This took into account the understanding of the concept of "restricted information", which was defined by one of the authors in his previous work;

the idea of the content of protection of restricted information is summarized, and also each of properties of the information which make the content of its protection is investigated.

Keywords: information security, information with limited access, content of information security, information properties.

DOI: https://doi.org/10.23856/4621

1. Introduction

In modern society, information appears, disappears, changes at a very rapid pace. Analysts, analytical software and data center networks do not keep up with the information. There is also information that has the features of creation, processing, transmission, destruction. The subjects of information relations are interested in ensuring the protection of this information. Such information in the Ukrainian legal system is classified as restricted information.

Under the law, national authorities are obliged to take appropriate legal measures to ensure the preservation of this information from the moment of creation, prevention of unauthorized destruction, distortion or access to it.

The analysis of the legislation of Ukraine showed that it does not even contain a definition of the term "protection of restricted information", given that it is possible only to get a general idea of such information.

Analysis of research and publications has shown that the issue of types of restricted information (secret, official and confidential information) is given enough attention by scientists. Also, public relations related to these types of restricted information are regulated by law, but there is legal uncertainty and inconsistency in the concepts of some types of protection of restricted information, which are found in legislation on the subject of research.

At the same time, the rules of law must be clear for their proper application in practice, and the lack of proper systematization of legislation, preparation of draft acts by various agencies results in a distorted understanding of the content of state-sanctioned rules of conduct, different interpretations.

Therefore, research on the protection of information, the content of the protection of restricted information and analysis of the basic terminology related to the protection of restricted information, on the example of Ukrainian legislation are relevant.

That's why, the purpose of the article is to highlight the results of the analysis of problematic issues to determine the content of the concept of protection of restricted information, in particular the results of analysis of existing terminology used by Ukrainian legislation on protection of restricted information.

2. The context of information security

The large explanatory dictionary of the Ukrainian language defines the word "context" in several meanings. However, for our study, we apply the understanding of meaning as a reasonable basis, purpose, appointment of something *(Busel, 2005).*

To understand the meaning of the protection of restricted information, consider the meaning of "protection of restricted information" through the availability of other concepts that are defined by law.

The legislation of Ukraine does not provide a definition of "protection of restricted information", but it contains several definitions of "protection of information". This will help us gain an understanding of the content of information security through the analysis of its concept.

Thus, the Law of Ukraine "On Information" stipulates that information protection is a set of legal, administrative, organizational, technical and other measures that ensure the safety, integrity of information and proper access to it *(Law № 2657-XII, Verkhovna Rada of Ukraine, 1992).*

Another definition of information protection is given in the Law of Ukraine "On Information Protection in Information and Telecommunication Systems", although it is used for a particular information system, but at the level of law defines information protection and for our study its analysis is necessary. This law stipulates that the protection of information in an information system is an activity aimed at preventing unauthorized actions with regard to information in such a system *(Law № 80/94-VR, Verkhovna Rada of Ukraine, 1994).*

Thus, we have two legislative definitions of the term "information protection". It is important for our study that these definitions are not identical, which will help us to better understand the legal nature of the concepts.

Therefore, the first meaning defines the protection of information as a set of certain measures. The law defines these measures as legal, administrative, organizational, technical and others, which indicates the generality of the meaning, ie the species branching of both methods of protection and types of information. Next, we determine from this meaning the purpose of such measures, ie the object to which such measures are directed, and hence the content of the concept itself 1 (based on the semantics of the word "content"). These measures should ensure the safety, integrity of information and proper access to it. That is, the law defines a number of measures that are taken by uncertain entities in order to ensure certain results and properties of information. These results and properties of information are: its preservation, integrity and accessibility, which in our opinion is excessive for the general concept of "information protection" in the basic information law, because in general it is inappropriate to define such a specific content given the wider range of information properties.

As for the other concept, the legislator defines the protection of information in the information system as a certain activity of unidentified entities, which aims to prevent unauthorized actions on information. An understanding of the term "unauthorized actions regarding information in the system" is also derived from the same act of legislation. Unauthorized actions on information in the system are understood as actions carried out in violation of the procedure for access to this information, established in accordance with the law.

That is, the purpose of information protection in an information system is to prevent actions that are carried out in violation of the procedure established by law for access to information in such a system.

Therefore, common to the objects of information protection in the definitions of "information protection" is to ensure proper access to information. Thus, in our opinion, the first meaning is broader in relation to the second meaning, which determines the protection of information in a particular system. Therefore, common to the objects of information protection in the definitions of "information protection" is to ensure proper access to information.

Both definitions correspond to the areas of application of legislation. However, we believe that the first definition gives a general idea of the protection of information and it should not specify the properties that will be protected, because the term does not reveal what kind of information will be protected in what way.

3. The concept of technical and cryptographic protection of information

Let's move on to the analysis of definitions of the types of information protection, which are reflected in the regulations. Let's start with the most, in our opinion, classically defined in the legislation of Ukraine types of protection of restricted information, namely technical and cryptographic protection of information. Thus, the definitions of "technical protection of information" and "cryptographic protection of information" are given in the Law of Ukraine "On protection of information in information and telecommunications systems", which states that both cryptographic protection of information and technical protection of information are types of information protection. However, technical protection of information is aimed at preventing leakage, destruction and blocking of information, violation of the integrity and mode of access to information through engineering measures and / or software and hardware. Cryptographic protection of information is realized by transforming information using special (key) data in order to hide / restore the meaning of information, confirm its authenticity, integrity, authorship, etc. *(Law № 80/94-VR, Verkhovna Rada of Ukraine, 1994).*

Analyzing the definitions given in this law, it is necessary to take into account the scope of its application, namely to pay attention to the fact that the definition of technical and cryptographic protections is given in relation to information (not necessarily with limited access) processed in information and telecommunication systems.

Regarding the definition of the types of information protection, which refers to the most normatively regulated type of restricted information – state secrets, the Law of Ukraine "On State Secrets" defines the following:

technical protection of classified information – a type of protection aimed at ensuring the engineering and technical measures of confidentiality, integrity and preventing the blocking of information;

cryptographic protection of classified information – a type of protection implemented by converting information using special data (key data) in order to hide (or restore) the content of information, confirm its authenticity, integrity, authorship, etc. *(Law № 3855-XII, Verkhovna Rada of Ukraine, 1994).*

It should be noted that the legislative definitions of cryptographic protection of information in different laws are in fact identical, but the definitions of the term "technical protection of information" are different, which indicates some inconsistency between legislative acts.

Systematic legal acts for cryptographic and technical protection of information are also Decrees of the President of Ukraine of May 22, 1998 № 505 "On Regulations on the procedure for cryptographic protection of information in Ukraine" and from September 27, 1999 № 1229 "On Regulations on technical protection of information" in Ukraine".

Thus, the Regulation on the Procedure for Cryptographic Protection of Information in Ukraine gives approximately the same understanding of the above concept of "cryptographic protection of information", but in the Regulation on technical protection of information in Ukraine the concept of "technical protection of information" differs significantly from the above.

The latter defines technical protection of information not as a type of protection, but as an activity aimed at ensuring such content – confidentiality, integrity and accessibility of information *(Decree № 1229, the President of Ukraine, 1999).* Note that this definition was primary in relation to the above-cited legislative definitions and became the basis for the future formation of a legislative understanding of the term "technical protection of information".

We paid attention on the fact that the first editions, in particular in 1994 of the laws of Ukraine "On State Secrets" and "On Protection of Information in Information and Telecommunication Systems" did not contain a definition of the terms of the studied types of information protection. In the future, with the development of legal relations in the field of restricted information protection, the conceptual framework of bylaws proved to be more flexible and more responsive to the needs of the area.

By the date of entry into force of the Law of Ukraine "On Amendments to the Law of Ukraine "On State Secrets" (ie until 26.10.1999), which initiated the legislative definition of technical protection of classified information (and cryptographic as well), such a term was already defined by the Concept of technical protection of information in Ukraine, and the Regulation on technical protection of information in Ukraine. That is, legislators, defining this term in the law, already had certain normative developments and ideas in order to express it as successfully and clearly as possible.

The Law of Ukraine "On Information Protection in Information and Telecommunication Systems" *(as amended by the Law of 31.05.2005 № 2594-IV)* only from 01.01.2006 gave an idea of technical and cryptographic protection of information. Therefore, the state initially

standardized the notion of types of protection of state secrets and only six years later defined the same notions for other types of restricted information.

In general, the difference in the legal definitions of this term, in our opinion, is dictated not only by the peculiarity of the legal regulation of public relations of each of the legislative acts, but also by the achievement of technical progress, the development of engineering thought.

The structure of both definitions is the same, both understand this phenomenon as a type of information protection, which through certain measures will ensure the preservation of certain properties of information. However, the differences are in the details, by which we mean the provision of certain properties of information, such as the content of protection, as well as the prevention of certain consequences for information as a result of technical protection of information. Thus, the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" stipulates that the properties of information to be preserved as a result of protection are its integrity and accessibility, and prevents such protection from undesirable effects on information such as leakage, destruction and blocking. In turn, the Law of Ukraine "On State Secrets" stipulates that the properties of information to be preserved as a result of protection – its confidentiality and integrity, and prevents such protection from blocking information. That is, these laws distinguish the properties of information to be preserved. For the former, integrity and accessibility are crucial, for the latter, integrity and confidentiality, and the difference in preventing adverse effects on information is that the former requires technical protection of information to prevent leakage, destruction and blocking, and the latter only blocking.

To obtain a normative understanding of these properties of information, we again refer to the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" and the Regulations on Technical Protection of Information in Ukraine, which provide an explanation of these properties.

Thus, confidentiality – the property of information to be protected from unauthorized access; integrity – the property of information to be protected from unauthorized distortion or destruction; accessibility – the property of information to be protected from unauthorized blocking *(Decree № 1229, the President of Ukraine, 1999).*

Regarding negative influences, the law stipulates that: blocking of information in the system – actions as a result of which access to information in the system is impossible; information leakage – the result of actions as a result of which information in the system becomes known or available to individuals and / or legal entities that do not have the right to access it; access to information in the system – the user gets the opportunity to process information in the system; destruction of information in the system – actions as a result of which the information in the system disappears; unauthorized actions regarding information in the system – actions carried out in violation of the procedure for access to this information, established in accordance with the law; violation of the integrity of information in the system – unauthorized actions against information in the system, as a result of which its content changes *(Law № 80/94-VR, Verkhovna Rada of Ukraine, 1994).*

Therefore, given such interpretations of concepts in the legislation, we conclude that the concept of "technical protection of information", given in the Law of Ukraine "On protection of information in Information and Telecommunications Systems", contains duplication, because providing such a property of information as accessibility makes it impossible unauthorized blocking of information, while preventing blocking of information – its availability is ensured.

Formally, the analyzed term indicates the prevention of violation of the access regime, which literally does not determine the preservation of the availability of information. However, given the above definition of the term "access to information in the system", and also given

that the law interprets "the procedure for access to information in the system" as a condition for the user to process information in the system and the rules of processing this information *(Law № 80/94-VR, Verkhovna Rada of Ukraine, 1994),* we can argue that the impossibility of violating the regime of access to information is a property of information, namely accessibility.

We consider such discrepancy to be the only one in the given concept.

It is possible to consider as a problematic issue the lack of mention in this definition of ensuring the property of information – confidentiality, ie to be protected from unauthorized access, because the law also defines issues of protection of restricted information *(Articles 4, 8).* In contrast, the Law of Ukraine "On State Secrets" defines the preservation of confidentiality of information in the content of its technical protection.

In this regard, it is worth mentioning the term "information leakage", ie a situation in which information becomes known or available to individuals and / or legal entities that do not have the right to do so. Thus, if the concept mentions the focus of technical protection of information to prevent leakage of information, then by default it indicates that this type of protection is aimed at ensuring confidentiality as a property of information.

In turn, we believe that the definition of technical protection of classified information is balanced for a specific area of legal regulation – the protection of state secrets (necessary and sufficient). The definition, which is not overloaded with inversions, clearly conveys the motive of the term, pointing to the main property of classified information that needs to be provided – confidentiality. However, the universality of the conceptual apparatus of laws must ensure uniform understanding of the definitions of one type of information protection and therefore there is still something for researchers to work on.

In general, the preservation of the properties of information, including restricted information, during its processing is an important content of protection, and ensuring a certain result (goal) of information protection is directly dependent on the properties of information. Thus, the impossibility of information leakage – is consistent with the property of information confidentiality; impossibility of destruction of information – agrees with the property of information integrity; impossibility of blocking information – is consistent with the property of information availability.

Let's look at the properties of information through the prism of the definition of "cryptographic protection of information". As we described above, the legislators agreed with the apt definition of the term provided for in the Regulation on the Procedure for Cryptographic Protection of Information in Ukraine *(Decree № 505, the President of Ukraine, 1998).* Thus, all the considered definitions indicate the need for confirmation as a result of such protection of the authenticity, integrity, authorship of information.

Thus, the legislation of Ukraine contains a number of definitions of types of information protection. Analysis of each definition allowed us to conclude that such properties of information as confidentiality, accessibility, integrity, authenticity and authorship are the meaning of information protection. In this case, the technical protection of information determines the content of the availability of integrity and confidentiality of information, and cryptographic – the authenticity, integrity and authorship.

4. The concept of cybersecurity

It is more difficult to analyze the concept of "cybersecurity", because the term itself does not contain a reference to information. Thus, cyber protection in the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (hereinafter – the Law on Cyber Security) means a

set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detection and protection cyber-attacks, elimination of their consequences, restoration of sustainability and reliability of functioning of communication, technological systems *(Law № 2163-VIII, Verkhovna Rada of Ukraine, 2017).*

Based on the meaning of the word "content", chosen by us to determine the content of the protection of information with limited access, cybersecurity measures are aimed (used for the purpose) at:

1) prevention of cyber incidents;

2) detection and protection against cyber-attacks, elimination of their consequences;

3) restoration of stability and reliability of functioning of communication, technological systems.

All areas of cyber defense do not formally indicate the information or its properties, but for analysis it is necessary to consider the concepts of the terms "cyber incident", "cyber-attack", "technological system", "communication systems". All of them are listed in the Cyber Security Act.

Cyber incident – an event or series of adverse events of unintentional nature (natural, technical, technological, erroneous, including due to human factors) and / or those that have signs of a possible (potential) cyberattack that threaten the security of electronic communications systems, control systems technological processes, create the probability of violation of the normal mode of operation of such systems (including disruption and / or blocking of the system, and / or unauthorized management of its resources), endanger the security (safety) of electronic information resources.

Cyberattack – directed (intentional) actions in cyberspace, which are carried out by means of electronic communications (including information and communication technologies, software and hardware, other technical and technological means and equipment) and aimed at achieving one or a combination of the following goals: violation confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and / or technological systems, obtaining unauthorized access to such resources; violation of security, sustainable, reliable and regular operation of communication and / or technological systems; use of the communication system, its resources and means of electronic communications to carry out cyberattacks on other objects of cyber protection.

Technological system – an automatic or automated system that is a set of equipment, means, complexes and systems of processing, transmission and reception, designed for organizational management and / or process control (including industrial, electronic, communication equipment, other technical and technological means) independently from the availability of system access to the Internet and / or other global data networks.

Communication systems – transmission, switching or routing systems, equipment and other resources (including passive network elements that allow the transmission of signals by wired, radio, optical or other electromagnetic means, mobile, satellite communication networks, electric cable networks in the part in which they are used for the purposes of signal transmission), providing electronic communications (transmission of electronic information resources), including means and devices communications, computers, other computer equipment, information and telecommunication systems that have access to the Internet and / or other global data transmission networks *(Law № 2163-VIII, Verkhovna Rada of Ukraine, 2017).*

Returning to the three areas of cybersecurity, we can identify them, taking into account the knowledge of the importance of the components of their content:

1) prevention of adverse events of unintentional nature that endanger the security (safety) of electronic information resources;

2) detection and protection against actions in cyberspace, which are aimed, in particular, at violating the confidentiality, integrity, availability of electronic information resources, as well as eliminating the consequences of such actions;

3) restoration of sustainability and reliability of operation: equipment and other resources that ensure the transfer of electronic information resources; a set of equipment, tools, complexes and systems for processing, transmission and reception.

The law on cybersecurity, by electronic information resources means any information created, recorded, processed or stored in digital or other intangible form by electronic, magnetic, electromagnetic, optical, software or other means.

Thus, electronic information resources in the sense of the Law are always information, and the purpose of cyber protection is to prevent adverse events that threaten the security of information, protection from actions in cyberspace, which are aimed at violating confidentiality, integrity, availability of information, restoration of resources. information, information processing, transmission and reception systems.

Therefore, the content of cybersecurity is: safety of information, protection of information in cyberspace from violation of its basic properties, restoring the stability and reliability of equipment, systems and resources in which such information circulates and / or performs certain operations.

Also, analyzing the concept of cybersecurity, we note that this is a type of protection (including) information, which is more extensive in relation to technical and cryptographic protection of information, because it, among other things, includes measures of these types of information protection. Hence, the content of cybersecurity also includes the protection of information in cyberspace from violating its confidentiality, integrity and accessibility.

5. Conclusions

Thus, our study of problematic issues of defining the content of protection of restricted information provided an opportunity to first formulate our own understanding and definition of the concept of "protection of restricted information", which we base the definition of "protection of information" and take into account, as well as the features of the content of the concept of "restricted information" derived by one of the authors *(Kots, 2019).*

Therefore, under the protection of information with limited access, we mean a set of legal, administrative, organizational, technical and other measures to ensure the confidentiality, integrity and accessibility of information, which in the manner prescribed by law is classified as secret, official or confidential.

In addition, we have identified gaps in national law that do not give the same view on the protection of information with limited access. It was also possible to determine the main properties of information, the provision of which, from the standpoint of Ukrainian legislation, is the content of its protection.

Therefore, it is established that the content of any information protection is to ensure the preservation of information properties. Most of the norms of the Ukrainian legislation on information protection analyzed by us determine that ensuring the confidentiality, integrity and accessibility of information with limited access is the essence of its protection.

The obtained results will contribute to further research of the factors that determine the features of the protection of restricted information and its legal regulation.

References

Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy [Large Explanatory Dictionary of the modern Ukrainian language]: 250000 / uklad. ta holov. red. V. T. Busel (2005). Irpin: Perun. – VIII, 1728 S. [in Ukrainian]

Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 № 2657-XII [On Information]. Kyiv: Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 48, st.650. [in Ukrainian]

Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 № 80/94-VR [On Protection of Information in Automated Systems]. Kyiv: Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31, st.286. [in Ukrainian]

Pro derzhavnu taiemnytsiu: Zakon Ukrainy vid 21.01.1994 № 3855-XII [On State Secret]. Kyiv: Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 16, st.93. [in Ukrainian]

Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the basic principles of cybersecurity in Ukraine]. Kyiv: Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403. [in Ukrainian]

Polozhennia pro tekhnichnyi zakhyst informatsii v Ukraini: Ukaz Prezydenta Ukrainy vid 27.09.1999 № 1229 [Regulations on technical protection of information in Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/1229/99.

Polozhennia pro poriadok zdiisnennia kryptohrafichnoho zakhystu informatsii v Ukraini: Ukaz Prezydenta Ukrainy vid 22.05.1998 № 505 [Regulations on the procedure for cryptographic protection of information in Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/505/98.

Kots D. V. (2019) Teoretyko-pravovi zasady informatsii z obmezhenym dostupom [Theoretical and legal foundations information with limited access]. Visnyk NTUU "KPI". Politolohiia. Sotsiolohiia. Pravo. Vypusk 2 (42). Kyiv: Helevetyka. S. 107–111. [in Ukrainian].