LEGAL BASIS OF ENSURING CYBER SECURITY OF UKRAINE: PROBLEMS AND WAYS OF ELIMINATING

Zinaida Zhyvko[1], Taras Rudyi[2], Volodymyr Senyk[3], Liliia Kucharska[4]

[1]*Doctor of Science (Economics), Professor, Department of Management, Lviv State University of Internal Affairs, Lviv, Ukraine, e-mail: professor2007@ukr.net, ORCID: https://orcid.org/0000-0002-4045-669X*

[2]*Ph.D. (Technical sciences), Associate Professor, Associate Professor of Department of Informatics, Lviv State University of Internal Affairs, Lviv, Ukraine, e-mail: tarasrudyy@gmail.com, ORCID: https://orcid.org/0000-0002-4106-4313*

[3]*Ph.D. (Technical sciences), Associate Professor, Head of Department of Informatics, Lviv State University of Internal Affairs, Lviv, Ukraine, e-mail: v.v.senyk@gmail.com, ORCID: https://orcid.org/0000-0002-0428-6443*

[4]*postgraduate, Lviv State University of Internal Affairs, Lviv, Ukraine, e-mail: liliia_kukharska@ukr.net, ORCID: https://orcid.org/0000-0002-8957-6983*

Citation:
Zhyvko, Z., Rudyi, T., Senyk, V., & Kucharska, L. (2020). Legal basis of ensuring cyber security of ukraine: problems and ways of eliminating. *Economics, Finance and Management Review*, (2), 82–90. https://doi.org/10.36690/2674-5208-2020-2-82

Received: April 27, 2020
Approved: May 30, 2020
Published: June 05, 2020

Abstract. *In the study we tested the analysis of modern data on cyber security in Ukraine, we highlighted the main aspects of the regulatory and legal support of the national information security. Identified key reported measures to counteract threats to state information security in the whole and in each individual type and the lack of practical implementation these activities. Found, that at the legislative level had been adopted only two documents on cyber security: Law of Ukraine on "Fundamentals of National Security of Ukraine", and the Decree of the President of Ukraine № 47/2017 of February 25, 2017 about des approved the Doctrine of Information Security of Ukraine. In these documents cyber security is given priority in the security system. Determined the main problems of ensuring the cyber security: ineffective regulatory and legal support and system of governance; the lack unified strategy of cyber security; low level of government management in cyber defense; temporal inconsistence of state regulation in information area and development of a legal system for the regulation in protection of critical infrastructure seams; the lack of transactional approach to the state cyber security governance by the state part; no requirement for security system(SIS); employment outdated standards. Offered the replacement of technical security information documents (TS ID), more effective and modern basic standards, establish industry standards for information security system (ISS). Amend the Law of Ukraine "Information security and telecommunication system" and provide a new approach of the method for confirming compliance of information system of information security requirements by establishing criteria for compliance; conduct regular audits to ensure compliance with the requirements and proper functioning of the security management process; conduct proven system of security information.*

For further development we propose to provide new approach of the method for confirming compliance of information system of information security requirements by establishing criteria for compliance. The purpose of such event is to legislate the requirements of the standards of the family of information security management system (ISMS) for certain categories of information, which is protected by the legislation of Ukraine.

Keywords: *information security, cyber security, standards, information and telecommunication systems, computer systems, certification, security management.*

JEL Classification: E58, G18, G29

Formulas: 0; fig.: 0; tabl.: 1; bibl.: 9

Introduction. Ukraine's path in developing its cyber security needs fundamental and urgent changes. It's not just the leaders' point of view of cyber defense. The need for change is confirmed by attacks on critical infrastructure, many other incidents that in recent years have created Ukraine's dubious reputation as one

of the main cyber-ranges (Yankovsky, 2019).

According to the formal features in Ukraine, there is a State policy in the field of information and cyberspace development, all the Presidents call for the development and formation of an information society in Ukraine. There are the laws of Ukraine: Law of Ukraine on "National Security" No 2469-VIII of June 21, 2018, Law of Ukraine "About the basic principles of ensuring cyber security of Ukraine No.2163-VIII of October 5, 2017"; the Decree of the President of Ukraine No. 47/2017 of February 25, 2017 approved the Doctrine of Information Security of Ukraine; the Resolution of the Cabinet of Ministers of Ukraine "Some questions of documentation of management activity" of January 17, 2018 No. 55; the Government approved "The concept of the development of the digital economy and society of Ukraine for 2018-2020" of January, 17, 2018 No.67- 2018; there are the Ministry of Internal Affairs, the Ministry of Justice, but it's impossible to see the real, positive results of presidential appeals, laws and ministries.

The legislation is an important component in ensuring information security (IS) and cybersecurity of the state, but it is time to move from words to action, given that the main fault of the current security legislation is its passive nature - declares only the need to ensure IS, cybersecurity and combating cybercrime at the level of doctrines, decrees, decisions, etc. That is, the "direction" to be followed in the absence of legal, financial and human support and without any responsibility of officials is set (Analytical note. National Institute of Strategic Studies, 2011).

Security of information and cyberspace, introduction of digitalization of management processes, guarantee of security and sustainable functioning of national critical infrastructure, information systems should become not only components of state policy in the field of cyberspace development and formation of information society in Ukraine, but also inclusion of these factors in political priorities (Rudy, T., Senyk, V., Rudy, A.& Senyk, S., 2018).

Literature review. Significant contribution to the solution of these problems at the theoretical level was made by such scientists as: V.L. Buryachok, V.O. Khoroshko, V.B. Tolubko, A.I. Marushchak, M.V. Hutsalyuk, K.V. Pestov, V.V. Kravchuk. The personalities of organizational and legal antidotes to cybercrime are devoted to the work of V.A. Lipkana, O.D. Dovganya, T.Yu. Tkachuk, V.S. Demedyuk, I.V. Krasnytsky.

Considering the results of the analysis of the literature sources of clear and understandable legal and regulatory documents and the organizational and legal measures to ensure the national system of cyber security, the information space of the state is not protected. We completely share the opinion of prof. Hrytsiuk Y.I. that there are no effective and efficient measures to prevent and counter cyber threats, and the existing ones are unsystematic and, as a result, useless.

Many of these publications concern the author's vision of the problems in the system of cybersecurity that cannot be solved without the introduction of new laws, regulations and new policies of the State in the sphere of digital security, that is, without considering information relations from the point of view of the object of the legal regulation (Rudy T., Senyk V., Rudy A. & Senyk S., 2018).

At the same time, despite the significant number of scientific publications on information-free issues, the rapid development of information technology (IT) the emergence of new ways and means of making cybercrime usable in the information field necessitates further research on the subject.

Aims. The purpose of the study, within the framework of this publication, is to analyze the reasons for the poor information and cyber security of the State in general and the problems of the inefficient legal and regulatory framework in particular, a number of systemic problems in the field of cybersecurity, which are becoming increasingly difficult to ignore.

That is, one of the main problems remains the inefficient regulatory framework and, above all, the lack of regulation of the information management system, should ensure the dynamics of the processes of legal provision of information and cyber security in Ukraine (Leonov & Serohin, 2019).

This state of affairs should lead to a profound change in the attitude of our state to the security of our own information and cyberspace, and hence to the information security (IS), its processing and the cyber-environment, in which this information circulates, the identification of targets, that is, prior to the adoption of information and cyber security measures.

Methods. In the study, scientists used methods of theoretical analysis and content analysis, monographic method, method of systematization to identify and specify the author's position within the studied issues. When preparing conclusions and recommendations based on the results of the study, the method of generalization was used.

Results. Outline of the main points. At the international and national levels, cybercrime is one of the most pressing challenges facing law enforcement agencies in all States today. There is still no systematic approach to countering cybercrime in the light of the current challenges and threats to information security (Kostenko, 2019).

Today, the first and only legislative acts in the field of combating cybercrime, as a strategic position at the highest political level is the Law of Ukraine on "Fundamentals of National Security of Ukraine", and the Decree of the President of Ukraine No.47/2017 of February 25, 2017 about des approved the Doctrine of Information Security of Ukraine of December 29, 2016. They have legislated the place of cybersecurity as a priority for government agencies and the government.

Subparagraph 2 of paragraph 3 of Article 8 of the Law stipulates that the functioning of the national cybersecurity system is ensured by creating a regulatory and terminological framework in the field of cybersecurity, harmonization of regulations in the field of electronic communications, information protection, information security and cybersecurity in accordance with international standards of the European Union and NATO (Leonov & Serohin, 2019).

It was expected that these documents would form the basis for the development in the short term of an effective, up-to-date legal and regulatory framework and a number of other legal and regulatory acts, which should play a key role in ensuring information and cybersecurity in Ukraine. However, despite the continued aggression

of the Russian Federation, the arrival of the new Government, unfortunately we have remained in the same place, there has been no progress in this important area.

1. Ineffective regulatory framework and management system. The current legislation of Ukraine still lacks scientific justification for conceptual definitions and formulations concerning information relations, and sometimes their complete absence. To date, there is no legislative definition of the basic term "information security", although this terminology is used in some laws.

The terminology used in the field of information technology demonstrates the lack of unity and ambiguous interpretations of many concepts, including key concepts (this also applies to section XVI of the Ukrainian Criminal Code, under which cybercrime is investigated in Ukraine). This is a serious impediment to both law-making in the information field and in law enforcement, as well as an indication of the lack of a systematic response to these problems.

The Law of Ukraine "About the basic principles of providing cyber security of Ukraine" defines the term "cybercrime". This term is not at all in line with the Criminal Code of Ukraine (CCU), which contains a separate section XVI "Criminal offenses related to the use of electronic computing machines (computers), system and computer network and telecommunication networks", where the term is used computer crime ″.

It is worth noting that the widespread use of so-called "communicators" and "smartphones", which combine the characteristics of mobile telephones and computers, has made cybercrime widespread, the content of which covers the whole spectrum of socially dangerous activities in the field of information technology (IT) (Leonov & Serohin, 2019).

Valid today are the normative definitions of the computing machine and the electronic computing machine that do not allow for the interpretation of modern terms and concepts of the IT sphere that correspond to their physical meaning or are too limited.

The authors share the idea set out in strengthening the response to cybercrime, including its organized forms, which includes (Hutsalyuk, 2019): considering the severe consequences that may result from the commission of cybercrime, initiate the strengthening of sanctions for the commission of offences under articles 361, 361-1, 361-2, 362, 363 and 363-1 of the Criminal Code of Ukraine; by supplementing these articles with the relevant parts, which will make it possible to transfer them to the category of serious crimes, increase criminal responsibility for their commission and expand the list of covert investigative (search) persons activities that can be undertaken to disrupt or document; strengthen public-private partnerships to counter cybercrime, including in the preparation of legal instruments in this area.

That is, the development and public discussion of amendments and additions to the Criminal and Administrative Law, in particular the expansion of Section XVI, is now a topical issue "Criminal offenses related to the use of electronic computing machines (computers), system and computer network and telecommunication networks" (Tarasyuk, 2019).

In Ukraine, unfortunately, there are no official state statistics that objectively reproduce information on cybercrime (reports on the commission of cybercrime are dispersed among various law enforcement agencies) which has a negative impact on precautionary measures that are fragmented, causing difficulties in counteracting and combating this type of socially dangerous act (Leonov & Serohin, 2019).

Thus, one of the main problems remains the inefficient legal and regulatory framework and, most importantly, the lack of regulation of the information management system, should ensure the dynamics of the processes of legal provision of information and cyber security in Ukraine.

However, it must be borne in mind that an important feature of the functioning of a State's information space is its high dynamism and the volatility of threats to IS This makes it impossible to establish an effective legal and institutional framework for IS for a period of more than 3-5 years, and for a real period of up to 2 years.

Therefore, at least every two years, existing legislation in this area requires adjustments to meet new challenges and threats, as well as changes in the geopolitical security environment, which is simply ignored in our state.

Account must also be taken of the fact that the development of information technology (IT), telecommunications systems, is taking place faster than the legal acts regulating them.

2. Transforming governance in cyber security. Ukraine's cyberspace is very vulnerable because there is no single unified cyber security strategy. The main cybersecurity challenges to be developed and implemented at the state level are as follows:

• protect cyberspace sovereignty and basic cybersecurity;

• critical infrastructure protection;

• development and implementation of digitization of public administration processes and on-line culture;

• countering cybercrime, espionage and terrorism;

• development of cyber-governance;

• strengthening international cooperation through the implementation in national legislation of individual legal acts adopted in the EU and NATO countries in the field of information protection, which are recognized at the state level by all countries.

All cyber security initiatives should be developed into a single transformation cyber security program. Such an approach is based on the development of a legal system for cyber security in Ukraine, which should be implemented in the normative legal support of current processes and expectations.

In order for the cyber security system to operate at the minimum necessary level, amendments to existing legislation are required, including the Law of Ukraine "On personal data protection", the Law "Fundamentals of National Security of Ukraine", etc.

Regulators in Ukraine are clearly lagging behind in developing a legal framework to regulate the security of critical infrastructure, as well as in providing content and regulations for framework laws on cyber security and cyber defense. The

development and adoption of a number of normative documents are relevant, in particular:

•requirements for cyber protection of critical infrastructure and assessment of cyber threats;

• audit of the state cybersecurity system (Kotlyarov, 2018).

The role of the state in the development of domestic cyber security also requires transformation. Obviously, this should not be a control function (as it is now), but rather a facilitative (organization of the process of collective problem solving) and assistance in solving cyber security problems (Kotlyarov, 2018).

In general, cyber security management in Ukraine at the state level is not effective. The national cybersecurity system is mainly limited to law enforcement. Private business and cyber speed are hardly involved in important issues.

As noted above, the lack of a transformational approach to national cyber security governance by the state implies the existence of an organization that will take over the management of the implementation of the cybersecurity program, and regular monitoring of the implementation process. That is, the regular monitoring of the program should be the responsibility of the non-governmental entity mandated to introduce cyber security reforms.

State structures limited to the current requirements of legislation and regulations will not be able to carry out such a transformation.

Another equally important issue is the lack of preparedness to respond to cyber incidents at the State level. Law enforcement agencies are still not organized for new waves of cyberattacks and do not have sufficiently trained professionals on their staff. There is also a lack of centralized management of cyber incident response forces at the state level.

In addition, it would be highly undesirable and possibly harmful for a State to follow a path in which the adoption of appropriate cyber protection requirements would require the approval of a draft technical regulation by a state institution. A second negative scenario in this process could be the references to procedures for the certification of integrated information security systems (IISS) (Kotlyarov, 2018).

3. Problems of certification of systems for security information. Let's try to clear the air a little bit. Ukraine has current law "Criminal offenses related to the use of electronic computing machines (computers), system and computer network and telecommunication networks" and has developed a series of regulatory documents for the system of technical protection of information, the main ones being the RD TSI 2.5-004-99 "Criteria for assessing the security of computer systems against unauthorized access". This document is used in the design and implementation of an integrated comprehensive information protection system (CIPS) for public information resources, as well as a special information system (SIS) in which information with limited access is processed, the requirement for the protection of which is determined by law.

At present, due to the lack of by-laws, the requirements for the protection of the special information system are hardly specified. The current provision of the Act "On the Protection of Information in Information and Telecommunications Systems" (art.

7), according to which State information resources or information with limited access, the requirement for the protection of which is established by law must be processed in the system using an integrated system of information protection with confirmed compliance.

That is, all systems are subject to this rule SI in SIS, their information infrastructure, requires compliance with the old standard of CIPS RD TSI 2.5-004-99.

The concept, internal structure and implementation model of the II SS do not meet the modern requirements for information security in the SIS, and the fact that this rule has not yet been removed from the legislation in force has been strongly criticized [3]. This is in line with current legislation, but with a very controversial approach, given the fundamental shortcomings and obsolescence of the concept of CIPS.

Moreover, they oblige public authorities, critical infrastructure and private companies that wish to provide services to public authorities (e.g., Internet service providers) to introduce CIPS. In addition to being obsolete, it has proven ineffective over the years (Dovgan & Tkachuk, 2019).

The immediate step is to replace the RD with a more effective and up-to-date basic standard and to introduce industry standards for SI systems.

This is not a new and creative proposal. We are looking for targets of low international standards, which registered themselves in the most developed countries of the world and the verified information. That is, there is a need for a transition to international security standards, which were previously consolidated.

This requires the adaptation of the new International Standard on Information Security Management Systems, or - to develop and develop its own, which new security standards for law enforcement services are unacceptable from time constraints and should be necessary.

Unlike the worldwide series ISO IEC 27000, which focuses on information security management, the information security criterion in RD TSI.

It is necessary to amend the Law of Ukraine "On the Protection of Information in Information and Telecommunications Systems" and to envisage a new approach to the way of confirming the compliance of the information system with the requirements for the protection of information by establishing appropriate criteria. The aim of such an exercise is to adopt in Ukraine the requirements of the standards of the Information Security Management System (ISMS) family of systems for individual categories of information, the protection of which is ensured by the legislation of Ukraine.

Certification of standards also requires regular audits to ensure compliance and proper functioning of the security management process. This narrows the gap that now exists between the various pieces of legislation and legislation, helps to convince regulators, and the organization constantly complies with the requirements of the legislation.

Certification according to the series ISO / IEC 270XX standard is carried out by certification bodies accredited by national accreditation organizations. In Ukraine, the National Accreditation Agency of Ukraine (NAAU) is such a state organization.

In accordance with paragraph 2 of the second part of Article 11 of the Law of Ukraine "On standardization", the decree of the Cabinet of Ministers of Ukraine No. 1163 dd. 26.11.2014 "On defining the state-owned enterprise to act as a National Standards Body", and pursuant to the Program of Work on National Standardization for 2019, national standards have been adopted, harmonized are European and international standards, the method of confirmation with effect from November 1, 2019 (Table 1).

Table 1. Ukrainian State Standards for Certification of Information Security Systems

№	ISO / IEC	Explanation
1.	DSTU ISO/IEC 27000:2016 (ISO/IEC 27000:2018, IDT)	Information technology — Security techniques — Information security management systems — Overview and vocabulary - to replace DSTU ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
2.	DSTU ISO/IEC 27001:2005 (ISO/IEC 27001:2013; Cor 1:2014, IDT) /Amendment N 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT)	Information technology — Security techniques — Information security management systems — Requirements
3.	DSTU ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Amendment N 2:2019 ISO/IEC 27002:2013/Cor 2:2015, IDT)	Information technology — Security techniques — Code of practice for information security controls
4.	DSTU ISO/IEC 27005:2018 (ISO/IEC 27005:2018, IDT)	Information technology — Security techniques — Information security risk management - to replace DSTU ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT)
5.	DSTU ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT)	Information technology — Security techniques — Guidelines for the assessment of information security controls -to replace DSTU ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT)
6.	ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) / Amendment N 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT)	Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Source: offered by the authors

Discussion. A separate problem area is SI system audits. In the ND coordinate system, only State-accredited organizations are authorized to carry out an audit. International IS and IT audit certificates are not yet recognized, which negatively affects audit quality.

Therefore, in order to comply with the legislation of Ukraine in the sphere of information security, it is advisable to introduce and, having passed a preliminary audit by a third party, to certify the ISMB in accordance with the requirements of ISO / IEC 27001. Since it is this standard that incorporates the world's best practices and methodologies, its implementation is used and recognized worldwide is the key to the system, to keeping the processes up to date and effective.

Conclusion. In accordance with the goal in the article was done as follows:

1. On the basis of the analysis, we believe that the existing legal framework, which, among other things, does not cover the full range of current threats to the cyber security of the state, should be substantially supplemented.

At the institutional and legal level, cyber security needs to be clearly identified and new, modern legal tools to counter these threats provided in a timely manner.

2. We propose to amend the Law of Ukraine "On the Protection of Information in Information and Telecommunications Systems" and to envisage a new approach to the method of confirmation of the compliance of the information system with the requirements for the protection of information by establishing appropriate criteria. The aim of this measure is to establish by law the requirements of the standards of the Information Security Management System (ISMS) family of systems for individual categories of information, the protection of which is ensured by the legislation of Ukraine.

Author contributions. The authors contributed equally.

Disclosure statement. The authors do not have any conflict of interest.

References:

1. Yankovsky, O. (2019). Ukraine needs a new cyber strategy. Retrieved from: https://www.pravda.com.ua/columns/2019/09/14/7226291/.

2. Problems of the current domestic legal and regulatory framework for combating cybercrime: the main directions of reform. Analytical note. *National Institute of Strategic Studies*. Retrieved from: http://www.niss.gov.ua/articles/454/.

3. Rudy, T.V., Senyk, V.V., Rudy, A.T. & Senyk, S.V. (2018). Organizational, legal, forensic and technical aspects of combating cybercrime in Ukraine. *Scientific Bulletin of Lviv State University of Internal Affairs. Legal series, 1,* 283-301.

4. Leonov, B.D. & Serohin, V.S. (n.d.). Challenges of legal and expert law enforcement in countering cybercrime. Retrieved from: http://academy.ssu.gov.ua/ua/page/page_1581430420.htm.

5. Kostenko, O.V. (2019). Problems of legal regulation and development of cyber security of Ukraine at the present stage. *Information and law. Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine, 3 (30),* 96-104.

6. Tarasyuk, A.V. (2019). Relationship between information and cyber security. *Information and law, 4 (31),* 73-82.

7. Hutsalyuk, M.V. (2019). Current trends in organized cybercrime. *Information and law. Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine, 1 (28),* 118-128.

8. Kotlyarov, Yu. (2018). Cybersecurity Law Architecture in Ukraine. Retrieved from: https: //www.reader.com/ukraine/yurydychna-gazeta/20180515/281578061307803

9. Dovgan, O.D. & Tkachuk, T.Yu. (2019). Conceptual framework for legislation Information security of Ukraine. *Information and law. Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine, 1 (28),* 86–99.