ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.41 Nº 76
Enero
Marzo
2023

Cuestiones Políticas Vol. 41, Nº 76 (2023), 419-436
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Application of international standards with a view to ensuring legal and organizational aspects of information protection in specialized information systems

DOI: https://doi.org/10.46398/cuestpol.4176.24

Sviatoslav Senyk *
Oleksandr Kondratiuk **
Ihor Fedchak ***
Stepan Tserkovnyk ****
Marianna Fedun *****

Abstract

The article analyzes the regulatory and legal framework of Ukraine in the field of information protection, in order to develop proposals on the improvement of organizational and legal measures aimed at the protection of information resources in specialized information systems of the state authorities of Ukraine. It was imposed the necessity to clearly identify at organizational and legal level the problems of safe operation of specialized information systems, to determine the key threats in the field of information protection and to provide in time new modern legal tools to counteract the threats. The need for reorganization and improvement of organizational and legal measures aimed at information protection was considered. Dialectical, hermeneutic, inductive and deductive methods of analysis and synthesis were used in the research. It was concluded that changing the legal framework in the field of information protection is a time challenge, and only the most rapid modernization of organizational and legal measures aimed at protecting information in specialized information systems will ensure the task of sustainable operation of specialized information systems.

* Doctor of Philosophy (Law), Associate Professor of Department of European Law, Ivan Franko National University of Lviv, Ukraine. ORCID ID: https://orcid.org/0000-0002-4187-9715

** Candidate of Legal Sciences, Associate Professor of Department of Operational and Investigative Activities, Lviv State University of Internal Affairs, Ukraine, ORCID ID: https://orcid.org/0000-0001-6102-2690

*** Candidate of Legal Sciences, Associate Professor of Department of Operational and Investigative Activities, Lviv State University of Internal Affairs, Ukraine, ORCID ID: https://orcid.org/0000-0002-4539-5988

**** Candidate of Legal Sciences, Senior Researcher of Department of Organization of Scientific Work, Lviv State University of Internal Affairs, Ukraine, ORCID ID: https://orcid.org/0000-0002-2293-1880

***** Candidate of Legal Sciences, Associate Professor of Department of European Law, Ivan Franko National University of Lviv, Ukraine, ORCID ID: https://orcid.org/0000-0001-9188-7142

Recibido el 14/10/22 Aceptado el 10/01/23

Keywords: information security; cybersecurity; specialized information systems; information resources; international legal standard.

Aplicación de normas internacionales con miras a garantizar los aspectos legales y organizativos de la protección de la información en los sistemas de información especializados

Resumen

El artículo analiza el marco regulatorio y legal de Ucrania en el campo de la protección de la información, con el fin de desarrollar propuestas sobre la mejora de las medidas organizativas y legales destinadas a la protección de los recursos de información en los sistemas de información especializados de las autoridades estatales de Ucrania. Se impuso la necesidad de identificar claramente a nivel organizativo y legal los problemas de funcionamiento seguro de los sistemas de información especializados, para determinar las amenazas clave en el campo de la protección de la información y proporcionar a tiempo nuevas herramientas legales modernas para contrarrestar las amenazas. Se considero la necesidad de reorganización y mejora de las medidas organizativas y legales destinadas a la protección de la información. En la investigación se utilizaron métodos dialécticos, hermenéuticos, inductivos y deductivos, de análisis y síntesis. Se llegó a la conclusión de que cambiar el marco legal en el campo de la protección de la información es un desafío de tiempo, y solo la modernización más rápida de las medidas organizativas y legales destinadas a proteger la información en los sistemas de información especializados, garantizará la tarea de la operación sostenible de sistemas de información especializados.

Palabras clave: seguridad de la información; ciberseguridad; sistemas de información especializados; recursos de información; estándar legal internacional.

Introduction

Development of the information and cyber space of Ukraine constitutes a key special feature of the future information technologies, and if Ukraine does not want to be left behind, it should already now, immediately, at an accelerated pace, respond to the changing threats, take specific steps to strengthen the state's information security. That is not just our view of the

current situation, but this idea is also confirmed by cyber-attacks against the critical infrastructural facilities, many other incidents that have made Ukraine disreputable as one of the key cyber grounds over the latest years (Yankovskyi, 2019).

Such status of cyber security in Ukraine has developed under the effect of a whole range of political, social and demographic, economic, legal, social and engineering, technological, and other factors. Superficial analysis of the situation, for instance, analysis of organizational as well as regulatory legal acts proves that in general the state is conducting an active and correct policy in the field of information security.

In particular, this is proven by the adoption of a number of regulatory legal acts over the recent years at the level of laws of Ukraine, decrees of the President of Ukraine, orders of the Cabinet of Ministers of Ukraine, orders of ministries and departments (On approval of the Concept of Developing Digital Economy and Society of Ukraine for 2018–2020 and approval of the action plan for its implementation, 2018; On the decision of the Council for National Security and Defense of Ukraine. On the Doctrine of Information Security of Ukraine, 2016; On the Main Principles of Ensuring Cyber Security of Ukraine, 2017; On the National Security of Ukraine, 2018); The strategy for the development of the system of the Ministry of Internal Affairs of Ukraine until 2020, 2017).

It was expected that these regulatory legal acts would become the basis for the development and implementation of effective organizational and legal measures that have to play a crucial role in ensuring information and cyber security in the state. However, analysis of actual results of application of their norms at the state level does not allow to talk about achievement of highly positive results. And sometimes even neglect of performance or compliance with the requirements of regulatory acts in the field of information and cyber security can be pointed out. Thus, it can be stated that the steps taken now in this domain that is important for Ukraine remain insufficient and ineffective.

Therefore, we can confidently state that ensuring of information and cyber security, reliable functioning of the national critical infrastructure, information and search as well as information and telecommunication systems must become not just a part of the state policy in the field of information protection, but must be included into the field of priority directions of the state policy. Hence, modern threats to information and cyber security require systemic response, adequate transformation of both the security sector in general and information and cyber security in particular already now (Rudyi *et al.*, 2018). In the same time should be taken into consideration relevant standards of the European Union (Gutnyk *et al.*, 2021).

One of directions of ensuring information and cyber security in Ukraine is organizing of ongoing monitoring of the global information security status, achievements in the field of information protection, that allowing to further ensure clear identification (at the organizational and legal level) of the problem of safe functioning of information and search as well as information and telecommunication systems, to determine key threats in the field of information protection and to ensure timely provision of new modern organizational and legal tools to counteract those threats, to meet the urgent need for reorganization and improvement of organizational and legal measures aimed at information protection in information and telecommunication systems.

Having said that, we cannot leave organizational and legal aspects of ensuring information security in sectoral specialized information systems (National Police of Ukraine, Security Service of Ukraine, Ministry of Defense, etc.) unattended. That is primarily related to the fact that mainly restricted-access information is processed in the information and search systems of those state entities. Therefore, development of new and improvement of current approaches to the implementation of those issues in the state's activity constitutes an important direction of ensuring its information and cyber security.

This article has been solving the following tasks:

- to conduct an analysis of regulatory documents that regulate issues of cyber security, information protection in information and telecommunication systems;
- to analyze international experience and international information security standards;
- to develop proposals for the implementation of international standards of information security to the existing legal framework in this field, primarily during the construction of complex information protection systems.

1. Literature Review

The results of analysis of a number scientific publications prove that the problems of legal regulation of organizational and legal measures aimed at information protection in specialized information systems constituted and still constitute an object of research for many experts. Some of them refer to the problems that cannot be solved if no new legislative, regulatory legal acts are introduced by the state in the field of digital space security, that is if information relations are not considered through the prism of the object of legal regulation (Rudyi *et al.*, 2017).

Here scientific achievements in this domain of such scientists as Buriachok, Tolubko, Toliupa, Khoroshko have to be mentioned. Special features of the organizational and legal principles of ensuring information security in specialized information systems are mentioned in the papers by Dovhan, Foros, Tkachuk, and others.

However, analysis of literature sources (Buriachok *et al.*, 2015; Foros, 2016; Dubov and Ozhevan, 2011) shows that no clear and totally comprehensible regulatory legal documents and organizational and legal measures aimed at ensuring existence of the national system of information and cyber security, protection of the state's information space, specialized information systems, computer networks have been finally developed.

There are no effective, efficient means of preventing and counteracting information threats, while the current ones are of no systemic nature and are, therefore, insufficient. The lion's share of information legal relations is regulated by by-laws, and sometimes even by departmental regulatory acts.

2. Methodology

The goal of this study is analysis of the applicable regulatory and legal provision of Ukraine in the field of cyber security, protection of information in information and telecommunication systems, development of proposals concerning improvement of organizational and legal measures aimed at information protection in specialized information systems with due account of the requirements of information standards on its basis.

Along with that, let us point it out that organizational and legal measures aimed at information protection in specialized information systems are considered as one of the strategic aspects of the system of information technology management in the state entities where restricted-access information is processed.

During scientific research, the use of the correct methodology is a guarantee that affects the result and quality of scientific work. The authors used the following main methods of scientific research: dialectical - gave an opportunity to consider the issue of cyber security as a process, the basis of which is the interaction, interdependence, mutual influence of various subjects, forms and methods and other components that take place in time and planes; hermeneutic, used to interpret relevant legal acts or their separate provisions, to establish the content of legislation and scientific knowledge taking into account the peculiarities of legal, legal and scientific language, when considering the categories of information space, information security; inductive and deductive - in the process of which a general conclusion about the results of the research is made on the basis of

the share of knowledge obtained; analysis and synthesis as interconnected and complementary methods, aimed at studying the existing methods of ensuring information protection in information and telecommunication systems, as well as during the study of regulatory and legal acts that regulate this field of activity.

The obtained data contributed to the formulation of the problem statement and research hypothesis as one of the methods of scientific knowledge.

3. State of organizational and legal support of information protection in specialized information systems of Ukraine

Lack of a systemic approach to the development of the state's legal policy in the information field also remains an important problem. A considerable drawback of the applicable Ukrainian legislation in this field, in particular, is lack of scientifically grounded definitions and wordings, and sometimes – their total non-availability. For instance, the applicable Ukrainian legislation does not have any clear definition of the notion 'information security' yet, though this notion may rather frequently be found in the regulatory legal documents regulating the issues of information protection.

The terminology applied in social relations in the field of information circulation often points to the lack of uniform, unambiguous approaches to the interpretation of many definitions, including the key ones. That refers, in particular, to Chapter XVI of the Criminal Code of Ukraine (Criminal offenses related to the use of electronic computing machines (computers), systems and computer networks and telecommunication networks) (Criminal Code of Ukraine, 2001), under which cyber crimes are investigated in Ukraine.

All that creates serious obstacles both for law-making activity in the information field, and for law-enforcement activity, as well as once again testifies to the lack of systemic nature in the settlement of the above issues (Dovhan and Tkachuk, 2019).

Thus, application of scientific methods of cognition, unified approaches to the development of conceptual principles in the field of information and cyber space protection, holding of analytical studies is a way capable of ensuring a real high-quality result, become the basis for passing further strategic decisions and determining the directions to improve regulatory legal, organizational and technical provision of cyber security in the state.

4. General analysis of the legislation of Ukraine in the field of information protection in information systems

Information relations constitute the basis of physical functioning of information and cyber space and therefore constitute the object of legal regulation. However, information technologies, telecommunication systems develop quicker than regulatory legal acts, by which they are regulated, are passed, which often constitutes the reason for the appearance of legal conflicts.

Current legislative base definitely is an important component in the implementation of information and cyber security of Ukraine. But it is high time that active actions be launched due to the fact that one of the key drawbacks of the applicable legislation in the security field is its passive nature, the need to ensure security of the information space and to counteract cyber crimes is only declared at the level of doctrines, decrees, decisions, etc. That is, the 'vector' that needs to be taken is set, while there is no financial, staff provision, no officials responsible for that are appointed, etc.

The legislation of Ukraine in the security field does not set the general frame approaches and directions, but sets detailed partial, step-by-step decisions. This statement is absolutely well-grounded and is accounted for, to our opinion, primarily by low level of training in the field of information technologies, the theory of information and cyber security of both officials assigned the duty of ensuring the state's information security, and specific performers dealing with the development of the regulatory legal base, and, most important – by the absence of the general state approach to ensuring sustainable functioning of the national critical information infrastructure.

Incorporation of Ukrainian legislation and the structure of regulatory legal acts of Ukraine in the field of information protection, that are binding as a legal doctrine, can be presented as follows: 1) Constitution of Ukraine; 2) laws of Ukraine; 3) decrees and orders of the President of Ukraine; 4) resolutions and orders of the Cabinet of Ministers of Ukraine; 5) regulatory legal acts of the Security Service of Ukraine, State Service for Special Communication and Information Protection of Ukraine; 6) international treaties of Ukraine related to information protection, consent to the mandatory compliance with which has been granted by the Verkhovna Rada of Ukraine. However, the problem of imperfect nature of the national legislation in the information field and absence of unified legal base related to ensuring information security in specialized information systems remains topical.

Among the key factors in this respect are regulatory factors – laws, standards, infrastructural decisions, etc. They aim at one common thing

– to ensure performance of organizational and technical guidelines, this enabling to raise the degree of protection of specialized information systems.

It should be pointed out that a significant progress has recently been made in the field of ensuring information and cyber security, in particular, at the institutional and organizational levels, in line with a number of regulatory legal documents (On approval of the Concept of Developing Digital Economy and Society of Ukraine for 2018–2020 and approval of the action plan for its implementation, 2018; On the decision of the Council for National Security and Defense of Ukraine. On the Doctrine of Information Security of Ukraine, 2016; On the Main Principles of Ensuring Cyber Security of Ukraine, 2017).

However, it should be taken into account that an important special feature of the information space functioning is its high dynamics and changeability of the threats posed to information security. That makes it impossible to develop effective organizational and legal provision in the field of information protection for the period longer that three – five years, and actually – even two years.

Therefore, at least every two years applicable legislation in this field will require adjustment in accordance with new challenges and threats as well as changes in the geopolitical security environment. Respectively, every two years information security policy in the bodies, institutions, enterprises processing information resources that are subject to protection must be reconsidered.

Such a situation causes changes in the treatment of security of its own information and cyber space by our state, and, hence, intensified protection of information, means of its processing and cyber environment in which this information circulates, identification of the objects under impact, that is taking measures to ensure information and cyber security (Yankovskyi, 2017).

Let us make an attempt to focus on the directions of improvement of organizational and legal measures aimed at information protection in specialized information systems where restricted-access information is processed with due account of special requirements set to security standards and independent audit of information security.

Currently, in Ukraine, besides the fundamental law On Information (1992), one of the key laws in the field of information protection is the Law of Ukraine on the Protection of Information in Information and Telecommunication Systems (1994). On their basis a series of regulatory documents for the system of technical information protection has been developed, of which the key one is ND TZI 2.5-004-99 (2012) The Criteria for Assessing Computer System Information Protection against Unauthorized Access. This document is used in the design and development

of comprehensive systems of information protection in state information resources as well as specialized information systems where restricted-access information protection of which is required by law is processed.

5. Discussion

Currently, due to lack of by-laws, requirements to the protection systems of specialized information systems are almost not specified. Now the norm of Art. 7 of the Law of Ukraine "On the Protection of Information in Information and Telecommunication Systems (1994)" still remains applicable. Under its provisions, state information resources or restricted-access information protection of which is required by law must be processed in the information system using a comprehensive information protection system of confirmed adequacy.

That is, all information protection systems in specialized information systems, their infrastructure requiring to comply with the requirements of the old standard for a comprehensive information protection system fall under the effect of this norm. However, the concept, inner structure and the model of implementation of a comprehensive information protection system, in fact, do not meet modern requirements to ensuring information security in specialized information systems, and the fact that this norm has not been removed from the applicable legislation is severely criticized (Yankovskyi, 2017).

In our opinion, the comprehensive information protection system currently contains the following drawbacks:

- outdated concept of information security system (it does not embrace the managerial level and security incident response, aims at protection and certification of information in some elements, and not in a specialized information system in general);
- does not ensure a sufficient degree of information protection system stable resistance to failures and restoration after failures;
- static nature and limited scaling opportunities (responding to incidents and threats posed to information security requires dynamic changes in the architecture of the protection system in real-time mode, which contradicts the paradigm of a comprehensive information protection system);
- large scale (considerable number of documents, confirmations and approvals).

Comprehensive information protection systems are not designed for risk-oriented approaches. They use the notions 'threat', 'vulnerability', and

do not take into account possible level of damages, related to compromising of a specialized information system (performance of the tasks assigned appears to be under threat and the possibility of unauthorized access to information assets of the specialized information system arises).

Therefore, implementation of a comprehensive information protection system is not accompanied by actual substantiation, which right away means implementation of ineffective solutions. Mandatory nature of the use of the comprehensive information protection system, under the law, is dictated not by the belonging of the object under protection, but by the mode of access to information assets.

In all aspects of ensuring information protection in specialized information systems analysis of possible threats to their failure, that is threats increasing vulnerability of information, lead to its leakage and unauthorized access, accidental or purposeful compromising, destruction, when it is impossible to establish a comprehensive information protection system, constitutes a key element.

Time has come to substantiate the development of organizational and legal measures aimed at information protection in specialized information systems, determining the strategy and tactic of the information protection system as well as taking into account the dynamics of changes in the threats to the information assets of the specialized information system.

With this in view it is necessary either to adjust current international information protection system standards, or to immediately develop and introduce own, qualitatively new security standards for the protection of information resources in specialized information systems.

Unlike a comprehensive information protection system, modern international information security standards must harmoniously be enacted within the organizational and legal structure, primarily, series of international standards ISO/IEC 27000, developed by the technical committee ISO/IEC JTC 1, subcommittee SC 27 of the International Organization for Standardization (ISO) jointly with the International Electrotechnical Commission (IEC).

Such approach to the modernization of organizational and legal measures of the information protection system in specialized information systems must be developed in accordance with the recommendations of international standards and in compliance with the provisions of the applicable Ukrainian legislation.

The critical criterion for information protection in ND TZI 2.5-004-99 (2012) is correspondence of the architecture and parameters of software and hardware means of a specialized information system to the regulations, that is, a comprehensive information protection system. Unlike it, the ISO/

IEC 27000 series of standards is the model to follow in the development, introduction, functioning, monitoring, analysis, support, and upgrading of the system of information security management.

Thus, currently, in Ukraine there have appeared two simultaneous paradigms of information protection systems: comprehensive information protection system and information security management system. Changing of the regulatory legal base in the field of information protection is the challenge of the times, and only as quick modernization of organizational and legal measures aimed at information protection in specialized information systems as possible will enable to ensure performance of the task set – sustainable functioning of specialized information systems.

In the conditions of implementation of the technology of systems with open architecture, that are distinguished for the complex interaction of information systems of different origin (interoperability), availability of problems with transfer of applied software between different platforms (mobility) and other special features, the issue of implementation of the system of information security management is becoming more and more important.

The standard (ISO/IEC 27000) allows to correctly organize the process of information asset protection and risk management for those assets. To control the quality of information security management, process the institute of certification has been introduced. The certificate has an international status.

Under the Law of Ukraine "On Standardization" (2014) and to perform the "Program of Works in National Standardization" (2017) the State Enterprise "Ukrainian Scientific-Research and Training Centre on the Problems of Standardization, Certification and Quality" has adopted state standards of Ukraine in the field of development and certification of information security management system, harmonized with international regulatory documents through confirmation. Let us outline the main of them:

- DSTU (State Standard of Ukraine) (ISO/IEC 15408-1:2017 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: introduction and general model;
- DSTU ISO/IEC 15408-2:2017 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components;
- DSTU ISO/IEC 27000:2017 Information technology – Security techniques – Information security management systems – Overview and vocabulary;

- DSTU ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements;
- DSTU ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls;
- DSTU ISO/IEC 27003:2018 Information technology – Security techniques –Information security management systems – Guidance;
- DSTU ISO/IEC 27004:2018 Information technology – Security techniques –Information security management – Monitoring, measurement, analysis and evaluation;
- DSTU ISO/IEC 27005:2015 Information technology – Security techniques – Information security risk management;
- DSTU ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems;
- DSTU ISO/IEC 27007:2018 Information technology – Security techniques – Guidelines for information security management systems auditing
- DSTU ISO/IEC 27008:2018 Information technology – Security techniques Guidelines for auditors on information security controls;
- DSTU ISO/IEC 27011:2018 Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations;
- DSTU ISO/IEC 11577:2017 Information technology – Open Systems Interconnection –Network layer security protocol;
- DSTU ISO/IEC 15408-3:2017 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

For the processes of information security management system, the model of cyclic process, which uses the principle of managing information security, has been applied, of which centralized administration is the core (takes into account the specificity of functioning of a specialized information system – compliance with the secrecy mode).

Analysis, assessment and management of risks should be made on the basis of the classical CIA model (confidentiality, integrity, availability). In particular: confidentiality – access to information assets exceptionally for officially authorized users in the minimum necessary scope; integrity – protection of accuracy/correctness and completeness of the information

assets of a specialized information system and information processing methods; availability – ensuring continuous access to the information and hardware assets of a specialized information system, services in accordance with the mandates and rights provided to users in the necessary scope.

There is a separate observability requirement – ensuring the principle of non-denial of committed actions. The formulated rules are recorded in the respective documents (documentation of the procedures constitutes one of the key requirements of the ISO 27001 standard) (Sereda *et al.*, 2017: 72).

It would also be expedient to briefly analyze new ISO/IEC 27035 Information technology – Security techniques – Information security incident management standard (New ISO/IEC Standard Will Help Cope with the Most Serious Information Security Risks. Information technology, 2016), providing practical recommendations on detection, registration, and assessment of information security violation incidents.

The standard is valid for a wide range of information security incidents, purposeful or accidental, caused by technical or physical reasons.

Information security incidents pose a threat for specialized information systems as the result of appearance of a possible threat of unauthorized access to information resources, failure of network services, interception of identifiers, web-site modification, theft of personal data, and other incidents, for example, such as increasing terrorist threats (Wojciechowski, 2017).

An awareness of the principles, models, procedures play a key role in complete understanding of this standard. Key element of the ideology of this standard is analysis of incidents aimed to determine what information resources of the specialized information system should be protected against what incidents and to what extent prospective losses should be assessed in qualitative and quantitative figures. A considerable number of threats can be reduced using the approach to information security incident management, described in this new international standard.

However, implementation of international standards in Ukraine for information protection in information and telecommunication systems of special designation is faced with a number of problems, of which audit of the information protection system is the key one. Permission for making such audit is granted only to the organizations possessing a license for carrying such activity, granted by the state.

And during the audit (at the stage of state examination (Senyk, 2018)) of a comprehensive information protection system in the information or information and telecommunication system of special designation international standards on information and cyber security are not applied, this having a negative impact on the results of the audit.

Therefore, in order to introduce international standards into the processes of development and putting of comprehensive information protection systems into operation in information and search as well as information and telecommunication systems of special designation there is a need to replace regulatory documents on technical protection of information with modern basic standards that will take into account the experience of a number of international standards that have earned a good reputation in developed countries of the world and have been tested by time. In this case it will be possible to carry out state accreditation of the information protection system on the basis of international standards.

Conclusions

Judging by the research done, we consider that current regulatory legal base in Ukraine does not embrace the whole spectrum of modern threats to information security and should, therefore, be substantially supplemented.

The current status of information and cyber security provision in Ukraine can be characterized as insufficient, this being caused by a number of organizational as well as regulatory legal factors. One of the key factors among them is non-availability of effective regulatory legal base in the system of information and cyber security management. There are the following organizational reasons therefor:

- lack of readiness of state entities and the state in general to adequately respond to cyber incidents. Currently, there is no state program for filling this gap in Ukraine. Cyber security management in the state is characterized by low level of professional community involvement in it, lack of transformational approach presupposing availability of entities responsible for the implementation of programs, strategies in cyber and information security, lack of control over their implementation;
- at the state level there is no effective entity responsible for cyber intelligence. Most frequently the state is warned about possible cyber incidents, sometimes even through mass media, private, volunteering, or international entities;
- information protection audit is conducted with no due account of the requirements of international standards, this having a negative impact on its quality;
- the level of staff training in Ukraine, in particular, for state entities, in the field of cyber security is insufficient. Profile education in information protection issues needs to be improved;

- currently there are no programs of cyber culture development in the society.

Currently, at the organizational and legal level it is necessary to clearly identify the problem of safe functioning of specialized information systems, to determine key threats in the field of information protection and to provide new, modern legal tools to counteract these threats in time. In order to ensure organizational and legal principles of information and cyber security at the state level it is expedient to establish a respective institute or body.

This can be done either at the level of the Council for National Security and Defense, or at the level of the advisory body of the President of Ukraine. It should include not just professionals from state authorities, but representatives of business, volunteering or professional communities. Such institution must ensure development of new regulatory legal acts in the field, give proposals concerning changes in the applicable legislation, develop recommendations on ensuring functioning of the national cyber security system, settle other issues requiring respective expert evaluation.

Along with that, improvement of the organizational and legal measures aimed at information protection in specialized information systems must be based on international standards, which, unlike Ukraine's regulatory documents, take the process of processing, accessing and preservation of information and not a comprehensive information protection system as the object of protection. With this in view it is necessary either to adjust ISO/IEC standards of series 27000, or – to develop own, qualitatively new standards of ensuring information protection in specialized information and telecommunication systems.

Bibliographic References

BURIACHOK, Volodymyr; TOLUBKO, Volodymyr; KHOROSHKO, Volodymyr; TOLIUPA, Sergii. 2015. Information and Cyber Security: Social and Technical Aspect. DUT. Kyiv, Ukraine.

CRIMINAL CODE OF UKRAINE. 2001. Available online. In: https://zakon.rada.gov.ua/laws/show/2341-14. Consultation date: 12/10/2022.

DOVHAN, Oleksandr; TKACHUK, Taras. 2019. "Conceptual Principles of Legislative Provision of Information Security of Ukraine" In: Information and Law. Vol. 1, No. 28, pp. 86–99.

DUBOV, Dmytro; OZHEVAN, Mykola. 2011, The Problems of Applicable Domestic Regulatory Legal Base in the Field of Cyber Crime Counteraction: Key Directions of the Reform: Analytical Note. Available

online. In: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-chinnoi-vitchiznyanoi-normativno-pravovoi-bazi-u-sferi. Consultation date: 12/09/2022.

FOROS, Hanna. 2016. "Legal Regulation of Cybercrime Counteraction" In: The State of Law. Vol. 24, pp. 164–169.

GUTNYK, Vitalii; BRATSUK, Ivan; BURAK, Stepan; ZUBAREVA, Antonina. 2021. "The concept of constitutional pluralism as the fundamental basis for the development of the European Union legal order" In: Revista de la Universidad del Zulia. Vol. 12, No. 34, pp. 361-378.

ND TZI 2.5-004-99. 2012. The Criteria for Assessing Computer System Information Protection against Unauthorized Access: approved by order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine 28 April, 1999 with amendments introduced under order of the Administration of the State Service for Special Communication and Information Protection of Ukraine No. 806. Available online. In: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf. Consultation date: 12/09/2022.

NEW ISO/IEC STANDARD WILL HELP COPE WITH THE MOST SERIOUS INFORMATION SECURITY RISKS: INFORMATION TECHNOLOGY. 2016. Available online. In: http://csm.kiev.ua/index.php?option=com_content&view=article&id=1068:-isoiec-&catid=41:2009-10-16-12-08-07&lang=uk&Itemid=. Consultation date: 12/09/2022.

ON APPROVAL OF THE CONCEPT OF DEVELOPING DIGITAL ECONOMY AND SOCIETY OF UKRAINE FOR 2018–2020 AND APPROVAL OF THE ACTION PLAN FOR ITS IMPLEMENTATION: ORDER OF THE CABINET OF MINISTERS OF UKRAINE. 2018. Available online. In: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80. Consultation date: 12/09/2022.

ON INFORMATION: LAW OF UKRAINE. 1992. Available online. In: http://zakon2.rada.gov.ua/laws/show/2657-12. Consultation date: 12/09/2022.

ON STANDARDIZATION: LAW OF UKRAINE. 2014. Available online. In: http://zakon.rada.gov.ua/laws/show/1315-18. Consultation date: 12/09/2022.

ON THE DECISION OF THE COUNCIL FOR NATIONAL SECURITY AND DEFENSE OF UKRAINE. ON THE DOCTRINE OF INFORMATION SECURITY OF UKRAINE: DECREE OF THE PRESIDENT OF

UKRAINE. 2016. Available online. In: https://www.president.gov.ua/documents/472017-21374. Consultation date: 12/09/2022.

ON THE MAIN PRINCIPLES OF ENSURING CYBER SECURITY OF UKRAINE: LAW OF UKRAINE. 2017. Available online. In: http://zakon.rada.gov.ua/laws/show/2163-19. Consultation date: 12/09/2022.

ON THE NATIONAL SECURITY OF UKRAINE. 2018. Available online. In: http://zakon.rada.gov.ua/laws/show/2469-19. Consultation date: 12/09/2022.

ON THE PROTECTION OF INFORMATION IN INFORMATION AND TELECOMMUNICATION SYSTEMS: LAW OF UKRAINE. 1994. Available online. In: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. Consultation date: 12/09/2022.

PROGRAM OF WORKS IN NATIONAL STANDARDIZATION. 2017. Available online. In: http://uas.gov.ua/standrarization/prohrama-robit-z-natsionalnoi-standa/. Consultation date: 12/09/2022.

RUDYI, Taras; SENYK, Volodymyr; RUDYI, Andrii; SENYK Sviatoslav. 2018. "Organizational and Legal, Criminalistic and Technical Aspects of Counteracting Cybercrime in Ukraine" In: Scientific Bulletin of Lviv State University of Internal Affairs. Law Series. Vol. 1, pp.283-301.

RUDYI, Taras; ZAKHAROVA, Oleksandra; SENYK, Volodymyr; SENYK, Sviatoslav; IZIO, Marta. 2017. "Organizational and Legal Support of Information System Protection of the Units of the National Police of Ukraine on the Basis of International Standards" In: Scientific Bulletin of Lviv State University of Internal Affairs. Law Series. Vol**.** 2, pp. 213-225.

SENYK, Sviatoslav. 2018. "The Study of Organizational Basics for Constructing Comprehensive Restricted-Access Information Protection Systems in the units of the National Police of Ukraine" In: Scientific Bulletin of Lviv State University of Internal Affairs. Law Series. Vol. 4, pp.180-189.

SEREDA, Valerii; ZHYVKO, Zinaida; RUDYI, Taras. 2017. "Regulatory Legal Aspects of Applying International Standards in the System of Company Security Management" In: Modern Problems of Computer Science in Management, Economy, Education and Overcoming of the Consequences of the Chernobyl Disaster (materials of the XVIth International Scientific Workshop. National Academy of Administration). Kyiv, Ukraine.

THE STRATEGY FOR THE DEVELOPMENT OF THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE UNTIL 2020: ORDER OF THE CABINET OF MINISTERS OF UKRAINE. **2017**.

Available online. In: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80#Text. Consultation date: 12/09/2022.

WOJCIECHOWSKI, Sebastian. 2017. "Contemporary Terrorism in The European Union – The Hydra Syndrome?" In: Przegląd Strategiczny. No. 10, pp.295-305.

YANKOVSKYI, Oleksii. 2017. "What Is Wrong with the Draft Law on Cyber Security and How to Improve It" Available online. In: http://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci. Consultation date: 04/10/2022.

YANKOVSKYI, Oleksii. 2019. "Ukraine Needs a New Cyber Strategy" Available online. In: https://www.pravda.com.ua/columns/2019/09/14/7226291/. Consultation date: 06/10/2022.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.41 Nº 76

Esta revista fue editada en formato digital y publicada en enero de 2023, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org