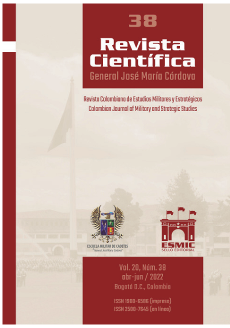
38
Revista Científica
General José María Córdova
Revista Colombiana de Estudios Militares y Estratégicos
Colombian Journal of Military and Strategic Studies
ESMIC
Vol. 20, Núm. 38
abr-jun / 2022
Bogotá D.C., Colombia
ISSN 1900-6586 (impreso)
ISSN 2500-7645 (en línea)

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

ISSN 1900-6586 (print), 2500-7645 (online)
Journal homepage: https://www.revistacientificaesmic.com

International and national standards on societal information security

Sofiia Lykhova
https://orcid.org/0000-0002-5678-5869
lykhova8138@edu.cn.ua
National Aviation University, Ukraine

Liudmyla Servatiuk
https://orcid.org/0000-0002-0315-8829
servatiuk8138@sci-univ.com
National Academy of the Security Service of Ukraine, Ukraine

Oleksandr Shamsutdinov
https://orcid.org/0000-0001-8820-4558
National Academy of the Security Service of Ukraine, Ukraine
shamsutdinov8138@neu.com.de

Viktoriia Sysoieva
https://orcid.org/0000-0001-7913-1676
sysoieva8138@acu-edu.cc
National Aviation University, Ukraine

Dariia Hurina
https://orcid.org/0000-0002-3692-4614
hurina8138@edu-knu.com
Ministry of Internal Affairs of Ukraine, Ukraine

How to cite in APA: Lykhova, S., Servatiuk, L., Shamsutdinov, O., Sysoieva, V., & Hurina, D. (2022). International and national standards on societal information security. *Revista Científica General José María Córdova, 20.* (38), 247-264.
https://dx.doi.org/10.21830/19006586.898

Published online: 2022

Submit your article to this journal:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL

Miles Doctus

ESMIC
SELLO EDITORIAL

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 247-264
https://dx.doi.org/10.21830/19006586.898

International and national standards on societal information security

Normas internacionales y nacionales sobre seguridad de la información en la sociedad

Sofiia Lykhova and Viktoriia Sysoieva
National Aviation University, Ukraine

Liudmyla Servatiuk and Oleksandr Shamsutdinov
National Academy of the Security Service of Ukraine, Ukraine

Dariia Hurina
Ministry of Internal Affairs of Ukraine, Ukraine

Abstract. This research focuses on information security as a social state, its aspects and characteristics, information security standards, and its impact on improving the information security process. It emphasizes the multidisciplinary nature of the issue of information security. Several methods are employed in this study, including formal-logical and system-structural methods, methods of generalization, and comparative law. Documentary analysis is used to examine the regulatory framework concerning information security and the main international and national information security standards. Three levels of information security are identified –personal, social, and state. It concludes that the levels differ depending on their degree within the information space.

Keywords: information space; information technology; policy management; public information; state security

Resumen. Esta investigación se enfoca en la seguridad de la información como estado social, sus aspectos y características, las normas de seguridad de la información y su impacto en la mejora del proceso de seguridad de la información. Hace énfasis en el carácter multidisciplinar de la seguridad de la información. El estudio emplea varios métodos, entre ellos el formal-lógico y el sistémico-estructural, los métodos de generalización y el derecho comparado. El análisis documental es utilizado para examinar el marco normativo de la seguridad de la información y las principales normas internacionales y nacionales en la materia. Se identifican tres niveles de seguridad de la información: la personal, la social y la estatal. Se concluye que los niveles difieren según su nivel dentro del espacio de la información.

Palabras clave: espacio informático; gestión de políticas; información pública; seguridad del Estado; tecnología de la información

Section: Dossier • Scientific and technological research article

Received: November 29, 2021 • Accepted: March 3, 2022

Contact: Sofiia Lykhova ✉ lykhova8138@edu.cn.ua

Introduction

Society has entered the era of global information relations. Consequently, safeguarding its information security is becoming the priority mission of modern states, along with protecting the national information space. However, the existing global and regional information confrontations, destructive communicative influences, the clash of multi-vector national information interests, and the spread of information expansion and aggression significantly complicate the fulfillment of this task and indicate the multifold nature of information security.

Information security is not a constant characteristic of a specific process or phenomenon. Its features include dynamism, multidimensionality, and uncertainty. Thus, developments concerning the management component and the technical characteristics of the information space, which provide for the study of this issue by technical disciplines, are constant. International standardization organizations, in particular, pay a great deal of attention to the information security management system. At the same time, legal sciences study many legal aspects of information security, particularly criminal, administrative, and civil law.

There is no consolidated view on the content of this concept in scientific literature, reiterating information security's multidimensionality. Thus, reducing information security to information protection is unbefitting; this concept is broader in nature. It is a multifold area of activity that requires a system-integrated approach. Defining information security requires determining its most essential features, considering the constant dynamics of information systems. It should be considered through the unity of signs such as state, features, and the management of threats and dangers, where the latter provides for choosing the optimal way to eliminate and minimize the impact of negative consequences (Galkin et al., 2020).

Ukrainian legislation defines *information security* as a state of protection of vital human, society, and state interests, preventing harm due to incompleteness, untimeliness, and unreliability of the information used; negative information impact; negative consequences of information technology use; unauthorized dissemination, use, and integrity violation, confidentiality, and information availability. The legislation on information should aim to consolidate the state's information policy. The policy should provide for a guaranteed level of national security in the information sphere, including a steady development of information technologies and protection tools, the exclusion of monopoly in this area, the prevention of the development of destructive information technologies, and the protection of copyrights.

Given that information and communication technologies are now used in all spheres of human life, there is an urgent need to ensure societal information security. A system of legal rules regulating relations in the information sphere is being developed to achieve and maintain an appropriate level of information security in society (Kniazieva et al., 2021). Moreover, state administration bodies' main directions of activity are being determined. Bodies and forces ensuring information security and a mechanism for monitoring their activities are being formed or transformed. To effectively ensure such security, it is important to approve its standards, which is a process that combines technical and legal components. This work is devoted to the legal aspects of the study of information security standards in society.

Due to the increased urgency of this problem, many domestic and foreign scientists have focused their research on information security. The legal aspect of the problem is particularly highlighted in works by Dovgan and Tkachuk (2019), Kuzmenko (2010), Marushchak (2010), and Ovsyannikov et al. (2015). These and other authors have made significant contributions to the development of information security. However, legal scholars continue to overlook the issue of standards for its provision.

The need for information security

This study was conducted using general scientific and specific scientific methods. The object of the article's research is presented, considering the research methodology. Three levels of methodology are generally accepted in legal research: fundamental (philosophical), general scientific, and specific scientific. With the help of the fundamental level of methodology, the most general principles and methods were ensured, which were further specified at the general scientific level.

The formal-logical, historical, system-structural, and generalization methods are worth noting among the general scientific methods used in the study. These methods are fundamental because they can be found in all fields of science and can help operations with the information presented in the research. The levels of information security and types of standards for its provision were identified using the system-structural method (Orlovskyi et al., 2018). The formal-logical method was used to analyze existing information security standards. Lastly, the positions of scientists on the researched problems were systematized and analyzed using the generalization method.

The study also used specific scientific methods, that is, methods specific to legal science, including comparative law, documentary, and statistics. To fully explore the delineated object, it is necessary to use the above methods comprehensively. The comparative legal method was used to analyze the regulatory framework for information security, and the documentary method was used to examine the international and national standards of information security.

The empirical basis of the study was examples of the application of international and national standards for information security by organizations, bodies, and institutions. The normative basis of the study included international regulations, Ukrainian legislation, and international and national standards in information security.

In the context of globalization and informatization, information security is becoming an urgent and critical task for every state. Ukraine is no exception. Even the Constitution of Ukraine (Article 17) states that ensuring information security is the State's most important function, a matter concerning the entire Ukrainian people (Constitution of Ukraine, 1996). In terms of solving this problem in Ukraine, several legal documents exist to firstly determine the general principles of information security and ways to improve it.

For example, the Law of Ukraine *On Basic Principles of Information Society Development in Ukraine for 2007-2015* defines the following ways to solve the problem of information security:

- Creating a fully functional State information infrastructure and ensuring the protection of its critical elements;
- Increasing the coordination level of State bodies' activities in identifying, assessing, and forecasting threats to information security, preventing such threats, and avoiding their consequences, as well as implementing international cooperation on these issues;
- Improving the information security regulatory framework, particularly in protecting information resources, combating computer crime, protecting personal data, and managing law enforcement activities in the information sphere;
- Deploying and developing the National system of confidential communication as a modern secure transport base capable of integrating territorially distributed information systems in which confidential information is processed (Law of Ukraine, 2007).

It is evident that the State is thorough in defining ways to ensure information security. However, it should be noted that information security as a phenomenon is not static. Just as information and communication technologies do not stand still, the state of protection of vital interests of man, society, and the state is constantly changing. Therefore, even if we can say that the state of information security has been achieved in a specific area at a specific time, it does not mean that this same condition will be maintained in subsequent periods. Information technologies are constantly evolving and improving, leading, among other things, to the emergence of new threats to information security. Therefore, it is necessary to pay attention to information security's instability. In addition, the state of security depends on many factors –both internal and external. The influence of these factors determines the presence or absence of information security.

However, it should be noted that such dynamism, multidimensionality, and uncertainty are not unique to information security. One must agree with the authors of the article, *The Negative Impact of Corruption on the Economic Security of States*. They rightly note that the threat to economic security is usually considered an undesirable but, at the same time, an integral part of the economic system, which operates in difficult competitive conditions, represented by a multifactorial, dynamic, and uncertain external environment (Akimova et al., 2020). All this indicates that information security standards cannot remain stable for a long time; they must be constantly revised, amended, and the old standards replaced by new ones.

Problems of scientific-theoretical reasoning

Kuzmenko (2010) distinguishes three levels of information security. They are as follows:

- Personal level (formation of rational, critical thinking based on the principles of freedom of choice);
- Social level (formation of high-quality information-analytical space, pluralism, multichannel information retrieval, and independent powerful mass media owned by domestic owners);
- State-level (information and analytical support of state bodies, information support of domestic and foreign policy at the interstate level, system of information protection with limited access, and counteraction to offenses in the information sphere –computer crimes).
- In turn, Ovsyannikov et al. (2015) consider information security as guaranteeing the state of security depending on the type of threats, which include:
- Individuals, society, state from the influence of poor-quality information;
- Information and information resources of the organization from the illegal influence of third parties;
- Information rights and freedoms of man and citizen.

These scientists noted that individuals' information security is characterized as a state of protection of the individual, various social groups, and associations of people from influences against their will and desire to change mental states and psychological characteristics, modify behavior, and restrict freedom of choice. State (society) information security is characterized by the degree of protection of the state (society) and the stability of the main spheres of life (economy, science, technosphere, management, and military affairs, among others); relatively dangerous information impacts (including destabilizing, destructive, and affecting state interests.) on the implementation and extraction of information. The State's information security is determined by the ability to neutralize such influences. Organization information security is the purposeful activity of its bodies and officials using permitted forces and means to achieve the organization's information environment's state of security, ensuring its normal functioning and dynamic development (Ovsyannikov et al., 2015).

In this regard, Marushchak (2010) adds that the problems of scientific and theoretical justification of the feasibility of legal regulation of public relations, arising from the information security of the individual, society, and state, are not only relevant; they are also practical. After all, for example, the regulation of relations on the dissemination of information on the Internet can occur both with the state's participation (both in China) and without legal influence. However, the level of protection of information interests of the state, and in many cases –society and individuals– may differ depending on the presence (absence) of legal regulation. Ensuring the safety of a person is very important in this aspect because an individual's life and health are the highest social value.

Guarantees for human security are a broad concept in which legal aspects are closely intertwined with philosophical, social, and even medical aspects. For example, the authors of the article, *Biomedical Ethics and Human Rights in the Context of Innovation and Information Development of Society*, note that biomedical ethics is a science of morality, through which human security guarantees are established, and moral and ethical barriers are created, supported by legal acts. The purpose of bioethics is to prevent harm to a person in need of medical care and protect rights and interests (Kalyuzhny et al., 2020; Vakulyk et al., 2020).

In determining the methods of legal regulation of public information and security relations, the conceptual difference between the principles of information security resources and the security of the state's information space should be considered. Marushchak (2010) considers these the main objects of information security, the basis of the information sovereignty of Ukraine. To ensure the security of the information space, it is necessary to strictly adhere to the constitutional principles of freedom of speech and the right to information. Meanwhile, to ensure the security of information resources, integrity, accessibility, and completeness of information are among the key aspects. Therefore, the method of legal regulation to ensure the security of information resources should be predominantly imperative, as it mainly concerns the protection of the right to information with limited access, while in ensuring the state's security of information space, it should be dispositive, as it relates to freedom of information, ways to obtain and disseminate information (Marushchak, 2010). In this work, we concede with the scientist's position on the delimitation of areas of regulation of public information and security relations. Indeed, significant restrictions on the rights and freedoms of citizens, especially in ensuring the security of the state's information space, will unlikely solve this problem entirely.

Information security is a component of the country's national security system. Ensuring the society's information security implies the protection of political, social, and economic interests. Given its importance, the international community has long heeded the development and improvement of standards for its provision (Chyzhmar et al., 2019).

Regarding information security standards, it is worth noting that the etymological meaning of the word *standard* is a norm or *sample*. On this matter, there is a broad and narrow interpretation of the term in science. In a broad sense, a standard is a particular sample, standard, or model against which other objects are compared and gauged. In the narrow sense, a standard is a normative or technical document that establishes norms, rules, and requirements for an object of standardization. Furthermore, it is worth considering this term's unregulated use in this sphere when analyzing the concept of information security standards.

The first problem that scientists face in studying the legal component of information security is defining *information security*. At the same time, one of the most controversial issues among scientists concerns information security. They recognize the state's interests in the information sphere and the information rights of citizens and society. However, they only recognize information security in information and telecommunications systems. Given the diversity in composition and content of information security objects, considering the leading scientists' positions on this issue is crucial. An important area of research involves determining the relationship of identical concepts used in current legislation that creates an ambiguous understanding of information security's structure. For example, the concept of *information security* is defined as the security of devices, processes, programs, environment, and data that ensure the integrity of information processed, stored, and transmitted. *Network security* is defined as measures to protect local computing networks from unauthorized interference with their functioning or attempts to disrupt the normal operation of its elements. The term *Automated System Data Security* (AS Data Security) is used to describe the quality of organizing access to data, protecting it from unauthorized use, intentional or unintentional distortion, or destruction. These definitions disagree with the definition of *information security* and the generic concept of *information security of telecommunications networks* as the ability of telecommunications networks to protect against destruction, distortion, blocking of information, or unauthorized leakage or violation of its routing (Marushchak, 2010). Unfortunately, this vagueness in terminology can lead to misinterpreting concepts.

Solodka (2013) notes that developed countries have established relations in this area, even before adopting legislation on personal data security. Ensuring proper protection of personal data is provided for in the EU-Ukraine Association Agenda, the EU Visa Liberalization Action Plan for Ukraine, and the draft of the EU-Ukraine Association Agreement. However, the legal institution of personal data in domestic information legislation is still in its infancy. Even after adopting the Law of Ukraine, *On Personal Data Protection*, Ukraine's legislation does not establish and, according to some scientists, cannot establish a well-defined list of information about an individual, the data considered personal, and how to apply the Law's provisions to various situations. This is particularly so when processing personal data in information (automated) databases and files of personal data that may arise in the future due to changes in public life. Under national law, personal data is information or a collection of information about an identified individual or one that can be specifically identified (Solodka, 2013). This definition does not improve specificity and may lead to a subjective interpretation in deciding whether a person's right to privacy has been violated.

In this regard, Ovsyannikov et al. (2015) draw attention in their article to the interests of the state in the information sphere. They include creating conditions for the harmonious development of the state's information infrastructure, implementing constitutional rights and freedoms of man and citizen in the interests of strengthening the constitutional order, upholding the country's sovereignty and territorial integrity, and establishing political and social stability, economic prosperity, unconditional implementation of laws, and support for international cooperation through partnership. The state carries out its activities through the relevant bodies, citizens, and public organizations and associations with the appropriate powers, according to the law. The state system is the most important part of the information security system of the individual, society, and the state. The main tasks of this system include detecting and forecasting destabilizing factors and information threats to the individual, society, and state's vital interests, implementing operational and long-term measures to prevent and eliminate them, and creating and maintaining forces (Ovsyannikov et al., 2015). Thus, State regulation of information security at all levels reflects the state of its provision. Ensuring information security depends on the national measures, whether the information and communication space will be protected, the citizens' security guarantees will be observed, and so on. At the state level, regulations are adopted to regulate this area of public relations.

There is also a position in legal science that maintains that the wording of the right to information and its restrictions (Articles 5, 6 of the Law, *On Information*, Article 6 of the Law, On *Access to Public Information*) do not meet international standards. Article 10 of the European Convention states that everyone has the right to freedom of expression. This right includes the freedom to hold opinions and receive and impart information and ideas without interference by public authorities and regardless of frontiers. However, these domestic laws do not address the exercise of the right to information irrespective of state borders; this is relevant in the age of the Internet. Furthermore, laws such as the Law of Ukraine *On Information*, *On State Secrets*, *On Access to Public Information*, *On Personal Data Protection*, and *On Banks and Banking* classify some information as *closed*, setting restrictions on the right of access to information. However, there are conflicts in these laws. For example, in the Law of Ukraine, *On Banks and Banking*, there is a conflict between the definition of *banking secrecy* and the list of information attributed to it. It should be noted that no list exists of information that can be classified as a trade secret; this complicates the exercise of a person's right to access information (Solodka, 2013). Thus, it can be stated that the Ukrainian national legislation has some gaps in the field of information security and regulation of public relations that arise in this sphere.

Dovhan and Tkachuk (2019) note that developing and adopting appropriate legislation is necessary to ensure information security. The basic principles of the construction of such a law, as well as information security activities, should firstly include the priority of human and civil rights and freedoms, a principle enshrined in International Law, reflecting the essence and limits of information security activities, and fundamental in the Doctrine of Information Security of Ukraine and observance of human rights and freedoms in the information sphere referring to the primary national interests of our country. The second principle involves the individual, society, and state's balance of interests. It is also provided by the Doctrine of Information Security of Ukraine. It follows the first because the legitimacy of each person's interests extends to the rights and freedoms of others and the interests of society and the state. These rights and freedoms ultimately caused the restrictions associated, for example, with the protection of state secrets and protection of personal data. The third principle, also following the previous principle, is the compliance of security measures with the degree of threats. Measures befitting the threats' actual level should be applied to prevent and eliminate them in the information sphere, with the minimum restrictions on the rights and freedoms of citizens. The fourth involves the state's monopoly on developing and producing special means of informational influence, including informational-psychological influence. In the conditions of Russian aggression, this means the prohibition in Ukraine of specific harmful information and inhumane informational-psychological technologies, which many lawyers rightly call information weapons. The fifth involves transparency and control of civil society in the field of information security. Namely, and following the Law of Ukraine *On Access to Public Information*, any information on the activities of public administration and local government to ensure information security is open and accessible to citizens unless they constitute a state secret or other secret provided by law. The last principle involves the obligation to involve public organizations in information security activities. This principle, which follows from the previous, and the principle of balanced interests of man, society, and the state, allows for public evaluation of bills related to the information sphere, fully taking into account the interests of various segments of the population to improve the quality of relevant legislation (Dovgan & Tkachuk, 2019). We acquiesce with the opinion of these scientists. Today, Ukraine has an urgent need to consolidate the general principles of information security at the legislative level. However, the development of such legislation should be approached with a clear understanding that information security is a dynamic, multifactorial phenomenon, and predicting how threats and challenges to information security will change in the future is challenging.

In the narrow sense, information security standards are represented by international and national standards of individual countries. Information security requirements to protect information or its properties are defined within the framework of international (ISO standards) and national standards (State Standards of Ukraine and Normative documents of technical information protection). In English standards, this is a classic Systemic-Institutional Alignment (SIA) model for ensuring the requirements of confidentiality, integrity, and availability of information. The requirement of observability (accountability) is made separately. The requirement of confidentiality applies to information; all others apply to both the information and the system as a whole. Three components are also considered for targeted application (protection and prevention mechanism) of information security standards within a certain model in information and telecommunication systems: hardware, software, and communication components (Ovsyannikov et al., 2015).

Organizations and standards to ensure information security

International standards of information security are normative documents developed by the International Organization for Standardization (ISO). The ISO is an independent, non-government organization made up of members from the national standards bodies of 165 countries. Its members play a vital role in how we operate, meeting once a year for a General Assembly that decides our strategic objectives. In Geneva, Switzerland, its Central Secretariat coordinates the system and runs day-to-day operations, overseen by the Secretary-General (International Organization for Standardization, 2021a). The ISO's primary goal was to promote international trade; however, the scope of its activities has expanded significantly with the development of information technology. To this end, this organization has developed the following standards to ensure information security:

- ISO/IEC 27033-3: 2010 *Information technology. Security techniques. Network security. Part 3: Reference networking scenarios. Threats, design techniques, and control issues*. It addresses the issues of possible threats, design and management methods, and possible threats for each scenario. It provides a detailed guide to dealing with security threats and the security and control design techniques needed to minimize the associated risks (International Organization for Standardization, 2010).
- ISO/IEC 27036-3:2013 *Information technology. Security techniques. Information security for supplier relationships. Part 3: Guidelines for information and commu-*

nication technology supply chain security. This document provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance on gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains. It also guides on responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks can be related to organizational as well as technical aspects (e.g., insertion of malicious code or presence of the counterfeit information technology (IT) products) and integrating information security processes and practices into the system and software lifecycle processes (International Organization for Standardization, 2013b).

- ISO/IEC WD 27036-1:2021 *Cybersecurity. Supplier relationships. Part 1: Overview and concepts*. This standard, as well as the previous one, concerns information security of information and communication technologies of the supply chain (International Organization for Standardization, 2021b).
- ISO/IEC 27002:2013 *Information technology. Security techniques. Code of practice for information security controls*. This document gives guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of controls considering the organization's information security risk environment(s). It is designed to be used by organizations that intend to: select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines (International Organization for Standardization, 2013a). It should be noted that this standard is currently in use, but another draft standard is being considered, which will replace this one.
- ISO/IEC TR 27016: 2014 *Information technology. Security techniques. Information security management. Organizational economics*. This document provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. This document is applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions (International Organization for Standardization, 2014).

- ISO/IEC 27035-3:2020 *Information technology. Information security incident management. Part 3: Guidelines for ICT incident response operations*. This document gives guidelines for information security incident response in ICT security operations. It does this by firstly covering the operational aspects in ICT security operations from a people, processes, and technology perspective. It then further focuses on information security incident response of ICT security operations, including information security incident detection, reporting, triage, analysis, response, containment, eradication, recovery, and conclusion (International Organization for Standardization, 2020).
- International standardization of the components of the information security management system forms three areas of development in this sphere:
- The group of standards: *Security Methods* - ISO/IEC 27000-ISO/IEC 27037;
- The group of standards *Methods and means of security* - ISO/IEC 15408 (*General criteria*, three parts), ISO/IEC 13335 (five parts), and ISO/IEC 18045;
- The group of standards *Management and audit of information technology* (CobIT, ITSM, ITIL, among others) (Ovsyannikov et al., 2015).
- In addition to the international standards developed by ISO specialists, there is a list of international cybersecurity standards developed by specialists of the British Standards Institute (BSI).
- BS 7799-1: 2005 — British standard BS 7799 first part. BS 7799 Part 1 is the Code of Practice for Information Security Management (Practical Rules for Information Security Management) describes the 127 control mechanisms needed to build an organization's information security management system based on the best examples of world experience in this field. This document is a practical guide to creating an information security management system.
- BS 7799-2: 2005 — British standard BS 7799 is the second part of the standard. BS 7799 Part - Information Security Management - The information security management system specification defines the specification of the information security management system. The second part of the standard is used as a criterion in the official certification procedure of the organization's information security management system.
- BS 7799-3: 2006 — British standard BS 7799 is the third part of the standard. A new standard in the field of information security risk management (Wikipedia, 2021).

These are the main international standards used by world organizations and institutions to ensure information security in their activities.

At the national level, many countries have developed their own information security standards, which are mandatory in a specific area. According to Ukrainian legislation, the standards of other countries may be applied in Ukraine in the prescribed manner by referencing them in national and other standards if their requirements do not contradict the legislation of Ukraine.

It is also possible to apply the official translation of international standards at the national level. For example, there is an identical translation of the relevant international standard in the State Standard DSTU ISO / IEC 27001: 2015 *Information technology. Methods of protection. Information security management systems. Requirements*. The specified State standard contains, among other things, a broad list of safety measures. These applicable measures include:

- Principles of information security management,
- Information security organizations,
- Security of human resources,
- Resource management of the information security management system,
- Access control,
- Cryptography,
- Physical security and infrastructure security,
- Operational safety,
- Communication security,
- Issues of acquisition, development, and maintenance of information systems,
- Relationships with suppliers,
- Information security incident management,
- Aspects of information security of business continuity management, and
- Compliance with certain requirements (National Standard of Ukraine, 2016).

According to Ovsyannikov et al. (2015), the application of the DSTU ISO/IEC 27001 for banking structures is mandatory and discretionary for structures with other activities. Additionally, harmonization is required with international standards ISO/IEC 27005: 2008 *Information Security Risk Management* and ISO/IEC 27003: 2010 *Guidelines for the implementation of information security management system* to implement the requirements of the information security management system in Ukraine. The first standard provides a framework for determining the approach to risk management depending on the scope of the information security management system, the scope of information security risk management or industry, and the process of information risk assessment, which involves the following two stages: 1) Information risk analysis (identify and quantify assets) - threats, existing means of control, vulnerabilities, and consequences; 2) Information risks assessment - risk management based on an iterative approach to its assessment to obtain an acceptable value. The second standard describes the information security management system's specification and design process from the beginning of the design to the submission of the plans for implementing the system. The purpose of the standard is to provide practical assistance in implementing the information security management system within the organization following ISO/IEC 27001: 2005. The Informatization Department of the National Bank of Ukraine implements the information security management system and risk assessment methodology based on the ISO/IEC 27003: 2010 standard, *Guidelines for implementing the information security management system* according to the National Bank of Ukraine's industry standards, considering the peculiarities of banking and requirements of the National Bank of Ukraine on information security (Ovsyannikov et al., 2015). These recommendations indicate that implementing information security management standards cannot be a one-off action. In fact, it is a continuous process of developing, implementing, operating, monitoring, reviewing, maintaining, and improving the information security management system. The *plan – execute – check – act* is applied in the modeling processes of the information security management system (National Bank of Ukraine, 2011). These recommendations determine the procedure for preparing the implementation of the information security management system, describing the existing infrastructure and security measures, and proposing risk analysis and assessment in the banking system of Ukraine.

Regarding other branches of management and societal life in general, the legal basis for information security (security of information resources) is contained in a system of documents, including the Constitution of Ukraine; Laws of Ukraine (*On Information*, *On the Protection of Information in Information and Telecommunication Systems*, *On Basic Principles of Information Society Development in Ukraine*, and *On Fundamentals of National Security of Ukraine*); Presidential and Cabinet of Ministers normative legal acts (National Security Strategy, Doctrine of Information Security of Ukraine, Concept of Technical Protection of Information in Ukraine, and Regulations on Technical Protection of Information in Ukraine); international and state standards defining the relationship between various ministries, agencies, and other Government agencies in terms of information security; and normative documents of the system of technical protection of information and departmental regulations within their responsibility. According to information security standards, an information and telecommunication system is considered protected if it meets the established requirements and guarantees for ensuring the confidentiality, integrity, accessibility, and monitoring of information assets. Undoubtedly, the scientists Ovsyannikov et al. (2015) are correct in stating that information security is a highly complex problem. Ensuring information security requires a comprehensive approach to security tools development at both the organizational and technical levels and management to provide a mechanism that allows the implementation of information security. Information security management is a part of the general management system whose purpose is to ensure the confidentiality, integrity, and accessibility of information assets (documents, media, applications, information systems, and staff knowledge). It implies implementing the company's security policy on an ongoing basis and its constant updating (Ovsyannikov et al., 2015). The previously mentioned documents primarily define the objects of protection involved in ensuring information security, how to analyze existing threats, challenges, risks, and most importantly, the security measures.

The development and implementation of information security standards are essential for creating a reliable and modern model for protecting personal data and information. Information security standards are designed to minimize risks and threats in the information space locally and internationally.

Conclusions

In conclusion, it should be noted that the information security problem is not limited to the technical or legal component. The information and communication spaces are not limited by state borders, and therefore ensuring information security is a strategic transnational task. In Ukraine, information security is ensured at the Constitutional level, providing for its protection. However, Ukraine merely entering the international system of information security standardization and certification is insufficient. National information security measures ensure the level of information and communication space protection; thus, regulations are adopted to regulate this area of public relations at the national level.

Because information security has a dynamic rather than static character, adopted standards do not remain relevant for long. The main international and national standards of information security considered in this work indicate that their approval is usually conditioned by the development of information technologies, the emergence of new information threats, and the increasing menace of information risks. Today, global information security is ensured through compliance with a number of international ISO standards, establishing the procedure for analysis and assessment of information risks and methods for combating them.

The adoption of the international standards and their supporting documents makes it possible to lay the foundations for implementing a new direction of standardization. In Ukraine, the development of a unified regulatory framework in information security can also ensure a high level of standards governing the conduct of certification tests and, as a result, increase confidence in the security of IT products and systems.

In addition to the analysis of information security standards, a comprehensive, system-forming legislative act that ensures a unified strategy for implementing state policy in the field of information security should be developed and enshrined at the legislative level.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Sofiia Lykhova received her Ph.D. in Legal Sciences in 2006. She graduated as a Professor of Criminal Law and Procedure in 2013. She is the Head of the Department of Criminal Law and Procedure of the National Aviation University.

https://orcid.org/0000-0002-5678-5869 - Contact: lykhova8138@edu.cn.ua

Liudmyla Servatiuk received a Ph.D. in Administrative Law and Process in 2009. She graduated as an Associate Professor of Constitutional, Administrative, and International Law. She has authored 44 scientific papers. She actively researches issues concerning the Ukrainian State Border Guard Service and other law enforcement agencies, national security issues, and border management.

https://orcid.org/0000-0002-0315-8829 - Contact: servatiuk8138@sci-univ.com

Oleksandr Shamsutdinov is a Professor at the National Academy of Security Service of Ukraine in Kyiv. He received an MS and Ph.D. in Law from the National Academy of Security Service of Ukraine in Kyiv. He is a researcher on Criminal Law, Information Safety and Security, and Biosecurity.

https://orcid.org/0000-0001-8820-4558 - Contact: shamsutdinov8138@neu.com.de

Viktoriia Sysoieva is an Associate Professor at the Department of Criminal Law and Process at the National Aviation University in Kyiv. Her expertise includes Law Enforcement and research work organization. She is a researcher on Criminal Law, current criminal law issues, modern crime detection factors, and crime prevention.

https://orcid.org/0000-0001-7913-1676 - Contact: sysoieva8138@acu-edu.cc

Dariia Hurina received Ph.D. in Law. She is the Deputy Head of the Laboratory of Educational and Scientific Work of the Ministry of Internal Affairs of Ukraine. Her expertise includes Law Enforcement, teaching, and research activities. Her research focuses include forensic examination, expert offense prevention, and accounting examination.

https://orcid.org/0000-0002-3692-4614 - Contact: hurina8138@edu-knu.com

References

Akimova, L., Litvinova, I., Ilchenko, H., Pomaza-Ponomarenko, A., & Yemets, O. (2020). The negative impact of corruption on the economic security of states. *International Journal of Management, 11*(5), 1058-1071. https://doi.org/10.34218/IJM.11.5.2020.097

Chyzhmar, Y., Rezvorovich, K., Orlovskyi, R., Kysylova, K., & Buhaichuk, K. (2019). State employment service: European approaches to providing electronic services. *Journal of Legal, Ethical and Regulatory Issues, 22*(6), 1-7.

Constitution of Ukraine. (1996). Law of Ukraine of 28.06.1996, No. 254k/96-VR. Article 7. Verkhovna Rada of Ukraine (Parliament of Ukraine). https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Dovgan, O.D., & Tkachuk, T.Yu. (2019). Conceptual principles of legislative support of information security of Ukraine. *Information and Law, 1*(28), 86-99. https://doi.org/10.37750/2616-6798.2019.1(28).221314

Galkin, A., Popova, Y., Kyselov, V., Kniazieva, T., Kutsenko, M., & Sokolova, N. (2020). Comparison of urban conventional delivery and green logistics solutions. Paper presented at the *Proceedings - International Conference on Developments in eSystems Engineering, DeSE, 2020-December* (pp. 95-99). Liverpool: Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/DeSE51703.2020.9450776

International Organization for Standardization (2021b). Cybersecurity. Supplier relationships. Part 1: Overview and concepts (SO/IEC 27036-1:2021). https://standards.iteh.ai/catalog/standards/iso/9bd-2dee7-5278-4b19-a629-1231f50ddfbe/iso-iec-27036-1-2021

International Organization for Standardization. (2010). *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues* (ISO/IEC 27033-3:2010). https://www.iso.org/standard/51582.html

International Organization for Standardization. (2013a). *Information technology. Security techniques. Code of practice for information security controls* (ISO/IEC 27002:2013). https://www.iso.org/ru/standard/54533.html

International Organization for Standardization. (2013b). *Information technology. Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security* (ISO/IEC 27036-3:2013). https://www.iso.org/ru/standard/59688.html

International Organization for Standardization. (2014). *Information technology. Security techniques — Information security management — Organizational economics* (ISO/IEC TR 27016:2014). https://www.iso.org/ru/standard/43756.html

International Organization for Standardization. (2020). *Information technology. Information security incident management — Part 3: Guidelines for ICT incident response operations* (ISO/IEC 27035-3:2020). https://www.iso.org/ru/standard/74033.html

International Organization for Standardization. (2021a). *About Us*. https://www.iso.org/about-us.html

Kalyuzhny, R., Макеіеva, O., & Shapenko, L. (2020). Biomedical ethics and human rights in the context of innovation and information development of society. *Journal of History Culture and Art Research*, *9*(1), 96-106. https://doi.org/10.7596/taksad.v9i1.2537

Kniazieva, T. V., Shevchenko, A. V., Shevchenko, A. V., Yaroshenko, O. M., Inshyn, M. I., & Yakovlyev, O. A. (2021). Current trends in the formation and development of insurance marketing in Ukraine. *Risk Management and Insurance Review, 24*(3), 279-292. DOI: 10.1111/rmir.12185

Kuzmenko, A.M. (2010). Peculiarities of problems of legislative provision of information security of the state, society and citizen in the conditions of information-psychological confrontation. *Journal of Kyiv University of Law, 4*, 317–321. http://kul.kiev.ua/images/chasop/2011_1/315.pdf

Law of Ukraine. (2007). No. 537-V. *On Basic Principles of Information Society Development in Ukraine for 2007–2015*. Verkhovna Rada of Ukraine http://zakon2.rada.gov.ua/laws/show/537-16.

Marushchak, A.I. (2010). Research of information security problems in legal science. *Legal Informatics, 3*(27), 17-21. http://ippi.org.ua/ai-marushchak-doslidzhennya-problem-informatsiinoi-bezpeki-u-yuridichnii-nautsi

National bank of Ukraine. (2011). Letter No. 24-112 / 365. *Regarding the implementation of the information security management system and risk assessment methodology in accordance with the standards of the National Bank of Ukraine*. https://zakon.rada.gov.ua/laws/show/v0365500-11#Text.

National Standard of Ukraine. (2016). *Methods of protection of the information security management system*. UkrNDC. https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

Orlovskyi, R., Shapoval, R., & Demenko, O. (2018). Possibilities of adapting the typologies of the international standards for establishing criminal liability for corruption-related crimes in Ukraine. *Journal of Eastern European and Central Asian Research, 5*(2). DOI: 10.15549/jeecar.v5i2.230

Ovsyannikov, V.V., Dekhtyar, S.V., Palamarchuk, S.A., Chernysh, Y.O., & Shemendyuk, O.V. (2015). Analysis of regulatory, legal, organizational, and technical aspects of information security. *Modern Information Technologies in the Sphere of Security and Defense, 3*(24), 187-193. https://doi.org/10.33099/2311-7249/2015-24-3-187-193

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues, 9*(3), 775-784. https://doi.org/10.9770/JSSI.2020.9.3(4)

Wikipedia. (2021). *BS 7799*. https://en.wikipedia.org/wiki/BS_7799