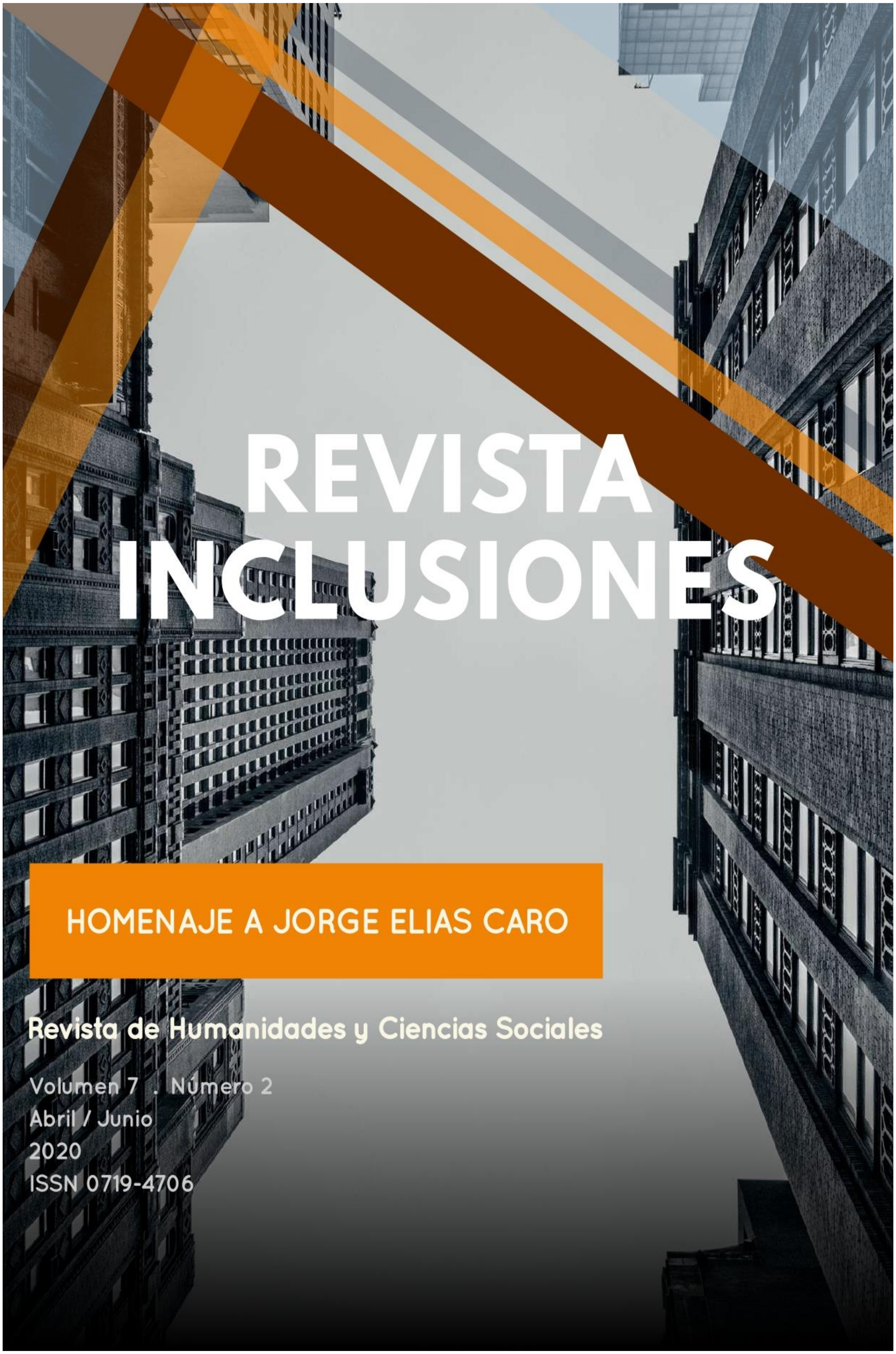

# REVISTA INCLUSIONES

HOMENAJE A JORGE ELIAS CARO

Revista de Humanidades y Ciencias Sociales

Volumen 7 . Número 2
Abril / Junio
2020
ISSN 0719-4706

REVISTA
INCLUSIONES
REVISTA DE HUMANIDADES
Y CIENCIAS SOCIALES

CUADERNOS DE SOFÍA
EDITORIAL

Editorial Cuadernos de Sofía
Santiago – Chile
Representante Legal
Juan Guillermo Estay Sepúlveda Editorial

**Indización, Repositorios y Bases de Datos Académicas**

Revista Inclusiones, se encuentra indizada en:

Web of Science Group
CLARIVATE ANALYTICS EMERGING SOURCES CITATION INDEX INDEXED
Clarivate Analytics
DOAJ DIRECTORY OF OPEN ACCESS JOURNALS
MIAR 2014 Live
latindex 15 años
CATÁLOGO
NSD ERIH PLUS EUROPEAN REFERENCE INDEX FOR THE HUMANITIES AND SOCIAL SCIENCES
PLATAFORMA Sucupira
CAPES QUALIS
INDEXED BY LatAm Estudios
Actualidad Iberoamericana
biblat Bibliografía Latinoamericana en revistas de investigación científica y social
CLASE Citas Latinoamericanas en Ciencias Sociales y Humanidades
CiteFactor Academic Scientific Journals
Academic Resource Index ResearchBib
WorldCat®
SHERPA/RoMEO
ROAD DIRECTORY OF OPEN ACCESS SCHOLARLY RESOURCES
PRINCETON UNIVERSITY LIBRARY
ubl
Stanford University LIBRARIES
Uniwersytet Wrocławski
uOttawa Bibliothèque Library
PARIS biu santé
WZB Berlin Social Science Center
TÜBİTAK ULAKBİM
VPL Vancouver Public Library
EST. 1785 UNB LIBRARIES
JÜLICH FORSCHUNGSZENTRUM
IPN

BIBLIOTECA UNIVERSIDAD DE CONCEPCIÓN

REVISTA INCLUSIONES
REVISTA DE HUMANIDADES Y CIENCIAS SOCIALES

CUADERNOS DE SOFÍA EDITORIAL

**ISSN 0719-4706 - Volumen 7 / Número 2 / Abril – Junio 2020 pp. 457-473**

# VALUE DETERMINANTS OF THE INFORMATION SECURITY OF A DEMOCRATIC STATE

**Dr. Oleg G. Danilyan**
Yaroslav Mudryi National Law University, Ukraine
ORCID: 0000-0001-5308-4664
odana@i.ua
**Dr. Aleksander P. Dzeban**
Yaroslav Mudryi National Law University, Ukraine
ORCID: 0000-0002-2075-7508
a_dzeban@ukr.net
**Dr. Yury Yu. Kalynovskyi**
Yaroslav Mudryi National Law University, Ukraine
ORCID: 0000-0002-0081-8107
kalina_uu@ukr.net
**Ph. D. Inna I. Kovalenko**
Yaroslav Mudryi National Law University, Ukraine
ORCID: 0000-0002-3156-9254
kinna087@gmail.com
**Ph. D. Julia V. Melyakova**
Yaroslav Mudryi National Law University, Ukraine
ORCID: 0000-0002-0200-1141
melyak77828@gmail.com
**Ph. D. Vadim O. Danilyan**
Ukrainian State University of Railway Transport, Ukraine
ORCID: 0000-0003-3469-9887
danilyanvadim@rambler.ru

**Fecha de Recepción**: 28 de enero de 2020 – **Fecha Revisión**: 06 de febrero de 2020

**Fecha de Aceptación**: 28 de febrero de 2020 – **Fecha de Publicación**: 01 de abril de 2020

## Abstract

This article analyses the information security of a modern democratic state in a value dimension. It is argued that spiritual values are a necessary component of strengthening the state's information security. The purpose of this work is to determine the essential characteristics of value determinants and to identify their taxonomy in the information security system of democratic countries. The ways of strengthening the information sovereignty of the state in the context of global competition and confrontation are analyzed. It is emphasized that the importance of strengthening the spiritual sphere of the state is determined by the widespread use of cyber terrorism, cyber espionage, information and hybrid wars in the modern world. The need for a clear fixation and reproduction of the axiological determinants of the information security of a democratic state is due, first of all, to the fact that one of the directions of information aggression, as a rule, is an active influence on the values of public and individual consciousness: their destruction, substitution, deformation. As a conclusion, it is noted that information is a strategic resource of the state, and the protection of the human and social rights to reliable information constitutes the value imperative of a democratic state. With the development of the information society, the world community is faced with the need to protect information human rights, counter information attacks, and form national information security systems.

**Keywords**

Information Security – Value Determinants – Democratic State – Information War – Information

**Para Citar este Artículo:**

Danilyan, Oleg G.; Dzeban, Aleksander P.; Kalynovskyi, Yury Yu.; Kovalenko, Inna I.; Melyakova, Julia V. y Danilyan, Vadim O. Value determinants of the information security of a democratic state. Revista Inclusiones Vol: 7 num 2 (2020): 457-473.

## Introduction

In the modern world, the problems of ensuring the information security of the state, society and a man are permanently relevant. The results of scientific and technological progress, improved information and communication technologies make it possible to penetrate into all spheres of the life of society and the state, to influence both positively and negatively on the processes in them. In the context of information confrontation at the global and local levels, the problem of protecting information and information and communication systems requires constant attention from the government bodies and civil society institutions.

In the context of our study, it should be noted that ensuring the information security of a democratic state has not only a technological, legal, political, but also a value-cultural dimension. It is mental structures, value determinants and imperatives of public consciousness that are the basis for protecting the state's information field and constitute a cognitive barrier against information aggression. It should be noted that in modern researches, the scientists quite rightly speak not only about information security, but also about a broader phenomenon - the spiritual security of an individual, society and the state.

Today, strengthening the information security of a democratic state presupposes the preservation and development of both national-cultural values and axiologemes that are democratic in nature - freedom, legal equality, justice, security, tolerance, solidarity, etc.

Based on the foregoing, the purpose of this work is to determine the place and the role of value determinants in the information security system, to identify their taxonomy, as well as the essential content in the practice of democratic countries.

## Methods

The problem of information security in the value dimension, from our point of view, cannot be comprehensively analyzed within the framework of the methodological potential of an individual science. In this regard, our study comprehensively applies both general scientific and philosophical methods, as well as the methods of individual sciences, namely jurisprudence, cultural studies, political science.

Thus, the comparative analysis method allowed us to show the differences in ensuring information security in different countries, to identify key values for the stable existence of various cultures and peoples. A complement to the previous method was the comparative legal method, the scientific potential of which was the basis for identifying the features of legislative support for information security in democratic states.

In turn, the method of the system analysis has become the key in determining the role and the place of information security in the structure of national security of the state. The dialectical method helped to identify contradictions in the value priorities of ensuring the information security of modern countries, in particular, Ukraine.

## Literature Review

In scientific literature, the problems of information security in general and in the value dimension in particular are presented quite widely. In this review, we will focus on those studies that have become the basis for our thoughts, hypotheses, and conclusions.

Thus, Yu. Kokarcha focuses on the problems of freedom in the virtual world, on those opportunities that the Internet provides for self-expression and communication. However, this scientist expresses concerns about the negative impact of information technology on a human[1].

In turn, French researchers K. Kerdellan and H. Hrezyion classify various threats to the information security of a person immersed in the virtual world[2]. In T. Kravchenko's scientific study, the value aspects of the activities of network communities are examined, the positive and negative aspects of their influence on the information security of the state are highlighted[3]. Ya. Liubyvyi points out that today the capabilities of Internet technologies are actively used by criminal groups, terrorist organizations, and the law-abiding citizens and public organizations that encounter illegal content can help the state to prevent such activities[4].

According to Yu. Dmyterko, the lack of development of legislation in this area and the ambiguity of interpretation of individual norms have a negative impact on the information security of the entities involved in virtual communication[5]. D. Protsenko reflects in the same vein, pointing out the need to classify the subjects of the Internet space, a clear definition of their rights and obligations[6].

From the point of view of I. Bushman, for the safe development of a democratic state, it is necessary to develop and constantly support basic values of social development[7]. Of course, without a value consensus, it is extremely difficult to strengthen the information security of a democratic political system. As O. Oliynyk points out, information security is a key element of the state's information sovereignty, these phenomena are in a dialectical relationship and determine the existence of each other[8].

A number of scientific works are devoted to the role of civil society in strengthening the information security of the state, the establishment of key democratic values in the public consciousness. Thus, K. Zakharenko, in his study, states that influential non-state

[1] Yu. A Kokarcha, “Internet yak chynnyk politychnoi sotsializatsii osobystosti v suchasnomu suspilstvi. Naukovyi chasopys NPU imeni M. P. Drahomanova”. Seriia 22: Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin, Scientific Journal of National Pedagogical Dragomanov University. Series 22. Political Sciences and Methods of Teaching Socio-Political Disciplines, issue 18 (2015): 80-86.

[2] K. Kerdellan y H. Hrezyion, Dety protsessora: Kak Ynternet y vydeoyhrы formyruiut zavtrashnykh vzroslыkh: [Per. s fr]. Ekaterinburg: U-Factor. 2006.

[3] Kravchenko, T. O. “Aksiolohichnyi aspekt informatsiino-merezhevoi paradyhmy. Filosofiia nauky: tradytsii ta innovatsii”, Philosophy of Science: Traditions and Innovations, num 1 (2010): 53-63.

[4] Ya. V. Liubyvyi, “Sotsialna refleksiia yak mekhanizm samoorhanizatsii sotsialnykh merezh. Multyversum. Filosofskyi almanakh#, Multiversum. Philosophical Almanac, issue num 1-2 (2016): 3-24.

[5] Yu. Yu. Dmyterko, “Vidobrazhennia diisnosti u ZMI: derzhavno-pravovyi aspekt zhurnalistyky. Efektyvnist derzhavnoho upravlinnia”, Efficiency of Public Administration, issue 38 (2014): 361-367.

[6] D. V. Protsenko, “Zakhyst prava na svobodu vyrazhennia v merezhi Internet: mizhnarodni tendentsii ta ukrainski realii. Naukovi zapysky NaUKMA. Yurydychni nauky”, NaUKMA Research Papers. Law, Vol: 144-145 (2013): 57-64.

[7] I. O. Bushman, “Tsinnisni oriientyry suchasnoho suspilstva. Hileia: naukovyi visnyk”, Gilea: Scientific Bulletin, issue 102 (2015): 201-205

[8] O. Oliynyk, “Informatsiynyy suverenitet yak vazhlyva umova zabezpechennya informatsiynoyi bezpeky Ukrayiny. Naukovi zapysky Instytutu zakonodavstva Verkhovnoyi Rady Ukrayiny”, Scientific notes the Institute of Legislation Verkhovna Rada of Ukraine, num 1 (2015): 54−59.

actors in the information security system are non-governmental analytical centers that develop and relay socially significant values[9]. At the same time, V. Lysak and O. Ageeva point to the insufficient willingness of state bodies to cooperate with analytical centers, to perceive them as influential and equal subjects of information security[10].

It is necessary to point out that applied aspects related to specific countries dominate in some studies on information security. For example, analyzing a number of problems related to the information security of the Ukrainian State in its axiological dimension, V. Khimei argues that they are caused by deformations of the information space under the influence of various objective and subjective factors[11]. Examining the problem of information security in Ghana, the researcher M. Evour points out that it is necessary to pay attention to the implementation of web portals, the creation of standards to maintain the interoperability of computer systems, the provision of a high-speed network for data exchange, the improvement of government employees' training engaged in information and communication technologies, as well as the enhancement of the security of government databases[12].

According to S. Kadir and S. Kwadri, when ensuring information security, the parties concerned should maintain the functioning of three main value attributes, namely confidentiality, integrity, and accessibility. Accessibility is the most critical attribute as the other two directly depend on it. After all, it is impossible to use the methods of confidentiality and integrity without accessible information[13]. In fact, the above specialists emphasize such important human rights (values) in the information sphere as protection of personal data, freedom to receive information, and reliability of information. Researchers M. Islama, J. Watsonb, R. Iannella and S. Geva demonstrate similar viewpoints on the problem of information security. In particular, they emphasize that confidentiality is not just concealment of information, but it also implies legal control over one's personal information[14]. Thus, the value of protecting the personal space as a condition for ensuring a citizen's information security is the most important factor in the development of a democratic state. Developing the above hypotheses, A. Veiga and N. Martins point out that the leaders of various communities can influence the culture of citizens by using different approaches to creating an environment where information is fully protected. The successful management of information security depends on the authority of the leader and effective management practices in this field[15].

[9] K. Zakharenko, "Efektyvnist vykorystannia potentsialu nederzhavnykh subiektiv informatsiinoi bezpeky. Multyversum. Filosofskyi almanakh", Multiversum. Philosophical Almanac, issue num 1–2 (2016): 58-70.

[10] V. F. Lysak y O. L. Ahyeyeva, "Suchasni ukrayins'ki "mozkovi tsentry" yak sub"yekty suspil'no-politychnoho protsesu v derzhavi. Hileya: naukovyy visnyk", Hilea: scientific journal, issue num 95 (2015): 380.

[11] V. Khimey, "Osnovni suchasni problemy informatsiynoyi bezpeky Ukrayiny. Tele- ta radiozhurnalistyka", Tele- and radio journalism, issue num 13 (2015): 127−132.

[12] S. K Ewurah, "The Concept of Government: ICT Policy Guidelines for the Policy Makers of Ghana", Journal of Information Security, num 8 (2017): 106-124.

[13] S. Qadir y S. Quadri, "Information Availability: An Insight into the Most Important Attribute of Information Security", Journal of Information Security, num 7 (2016).

[14] M. Islama; J. Watsonb; R. Iannella y S. Geva, "A greater understanding of social networks privacy requirements: The user perspective", Journal of information security and application, num 33 (2017): 30-44.

[15] A. Veiga y N. Martins, "Defining and identifying dominant information security cultures and subcultures", Computers & Security, num 70 (2017): 72-94.

According to N. Safa and C. Maple, information (computer) literacy is a key element in ensuring information security. The improvement of the level of users' awareness requires high-quality training in information security. The use of official presentations, games, Internet pages, e-mail, meetings and posters for these purposes showed that they constitute the key methods of increasing people's awareness[16]. Accordingly, sharing knowledge plays an important role in the field of information security, which is related to the fact that it has a positive effect on people's awareness. It is generally accepted that awareness of the risks in the information sphere is the most important factor that reduces the level of violations of the information security of a citizen, society and state[17]. It is possible to argue that a high-level awareness of the information and communication field allows all subjects of information security to understand and maintain the value aspects of personal and social being.

According to a number of researchers (N. Safa, R. von Solms and others), information security is still a complex issue for private users and organizations, which is related to the fact that information security is multifaceted and includes the protection of information from unauthorized access, disclosure, use, modification, malfunction, verification and perusal[18]. N. Safa, R. von Solms and S. Furnell rightly argue that although web technologies brought a number of benefits to different organizations and their clients, the problem of information security infringement still remains relevant. Antivirus, antispam, antifishing, antispyware, firewalls, authentication and intrusion detection systems constitute the technological aspect aimed at information protection. However, they cannot guarantee a safe environment for information[19].

Many authors (F. Belanger, C. Collignon, K. Enget, E. Negangard) come to the conclusion that information is one of the most valuable assets for any modern organization. That is why organizations focus on preserving security and improving their information systems due to the quantitative and qualitative intensification of security threats related to cyber-infection[20]. It can be argued that values are an essential component of ensuring the information security of a modern democratic state. This conclusion is confirmed by a variety of studies, some of which are reflected in the above review of scientific literature. At the same time, it is worth emphasizing the fragmented approach of scientists to the problems of the value determinants of information security, the insufficient identification of their influence on strengthening the information and cultural space of democratic countries.

## Results and Discussions

In the modern world, information is a key resource that forms the foundation of progress of a state, allows it to compete on the world stage, to occupy leading positions in geopolitical, economic and cultural spaces.

[16] N, Safa y C. Maple, “Human errors in the information security realm − and how to fix them”. Computer fraud and security, num 9 (2016).

[17] N. Safa; R. Solms y L. Futcher, “Human aspects of information security in organizations”. Computer fraud and security, num 2 (2016): 15-18.

[18] N. Safa, y R. Solms, “An information security knowledge sharing model in organizations”. Computers in Human Behavior, num 57 (2016): 442-451.

[19] N. Safa; R. Solms y St. Furnell, “Information security policy compliance model in organizations”, Computers & Security, num 56 (2016): 70-82.

[20] F. Belanger; St. Collignon; K. Enget y E. Negangard, “Determinants of early conformance with information security policies”, Information and Management, num 54 (2017).

Obviously, the human right to information is the basic legal value that a democratic state should protect. According to experts, the right to information is the individual's right to communicate, i.e. the expression of one's individuality in a society, which is one of the most important human rights. It is necessary to distinguish at least three aspects of modern information and communication relations, namely the ideological, technological, and information aspects[21].

Proceeding from the foregoing, it is possible to state that providing the right to information and ensuring the information security of an individual, the society and the state is a most relevant task. Such actualization is greatly strengthened due to information wars on our planet.

According to a number of scientists, the goal of information wars that currently pose a threat to each country is the establishment of the dominant position of a single state (or a group of states) over another in the information sphere, as well as the direct or indirect influence on the state's opponents by using the available information resources with the aim of controlling their actions. As a rule, the elimination of the consequences of information attacks requires huge intellectual and material investments, as well as a large amount of time for the restoration of affected areas in information systems[22].

According to the authors of this research, in addition to being a manifestation of economic, political, cultural and religious confrontation, information wars reflect the value differences in cultures, civilizations, peoples, and political and legal systems. In this regard, the development and implementation of axiological determinants of information security is a necessary foundation for the existence of the phenomenon under study.

The researchers D. Ki-Aries and S. Failye rightfully assert that information security issues are now widespread problems for a lot of organizations and institutions, especially in cases when the quality of information protection directly affects the regulatory or reputational aspects of activities. Therefore, companies strive to prevent intrusion into their information systems and data loss. At the same time, business can no longer rely exclusively on technologies to reduce risks in information security issues and requires all stakeholders' integrated efforts in the process[23].

In connection with the main hypothesis of this research, it is necessary to point out that the problem of protecting various subjects' information rights as one of the key values of a democratic state requires an adequate solution (reformatting) at the legislative level, which is related to new threats in the communication and information sphere.

As a matter of fact, information security has become a decisive factor in the survival of different institutions. Experts developed several security solutions aimed at minimizing the risks that threaten the activities of institutions, as well as maintaining confidentiality, integrity and accessibility of information. These solutions mainly focus on analyzing the

[21] O. Radchenko y O. Bukhtatyy, "Modelyuvannya derzhavnoyi komunikatyvnoyi polityky v umovakh suchasnoyi Ukrayiny. Publichne upravlinnya: teoriya ta praktyka", Public administration: theory and practice, issue 3 (2014).

[22] A. Pernebekova y A. Beisenkulov, "Information Security and the Theory of Unfaithful Information", Journal of Information Security, num 6 (2015).

[23] D. Ki-Aries y S. Failyє, "Persona-Centred Information Security Awareness", Computers & Security, num 70 (2017).

threats to information systems and the dangers of implementing countermeasures that reduce risks to an acceptable level[24].

Consequently, information is a strategic resource of a state, and the protection of people's and the society's right to reliable information is the value imperative of a democratic state. With the development of the information society, the world faced the need to protect people's information rights, to counteract information attacks, and to form national security systems. In 1986, European countries jointly developed common "Information Technology Security Evaluation Criteria" that served as a basis for the formulation of objectives in the field of information security, namely protecting information resources from unauthorized access for the purpose of ensuring confidentiality, ensuring the integrity of information resources by protecting them against unauthorized modification or destruction, and ensuring the operability of systems by countering the threats of service denial[25].

Reflecting on the nature of the axiological basis of information security, specialists distinguish a number of aspects for the examination of this problem. In particular, the researcher I. Ziaziun points out that the problem of axiological security, one of the important aspects of information security, is more relevant than ever. The author is convinced that very few people are actually aware of the real threat of axiological warfare. Structurally, values constitute the very citizenship and the very subjectivity of an individual. Therefore, the destruction of values affects all the areas of the life of an individual and the society[26].

Analyzing the viewpoints of I. Ziaziun, the authors of this research draw a conclusion about the persuasiveness of arguments related to the use of innovative terminology, namely "axiological security" and "axiological war". These concepts extremely accurately convey the essence of value confrontation in information wars taking place on our planet.

In modern conditions, networked communities and organizations play a special role in the formation of the value basis of social and state being and are accordingly considered the subjects of the state's information security. T. Kravchenko summarizes various sources and points out that there already exists a network organization of social life that consists in attracting many people to networked communities, whose communicative basis is the Internet. Networked communities are characterized by features that affect an individual's and the society's world of values, which in turn is reflected in the quality indicators of a state's information security. According to specialists, the negative features include uncertainty in information security of personal data in the network and the right of state structures to view the information of social network accounts; the possibility of destroying the life world of people, their life priorities and values by information technologies, and the "inclusion" of people's consciousness in a virtual reality that is dangerous to the psyche while information acquires the status of a universal civilizational value and a significant and vital resource of the society and the state[27].

[24] A. Gusmão; L. Silva; M. Silva; T. Poleto y A. Costa "Information security risk analysis model using fuzzy decision theory", International Journal of Information Management, num 36 (2016).

[25] A. A. Chichanovskyi y O. H. Starish, Informatsiini protsesy v strukturi svitovykh komunikatsiinykh system (Kyiv: Hramota, 2010).

[26] I. Ziaziun, "Kryza tsinnostei – katastrofa suspilstv i derzhav. Osvita doroslykh: teoriia, dosvid, perspektyvy", Adult Education: Theory, Experience, Perspectives, num 2 (2010).

[27] T. O. Kravchenko, "Aksiolohichnyi aspekt informatsiino-merezhevoi paradyhmy. Filosofiia nauky: tradytsii ta innovatsii", Philosophy of Science: Traditions and Innovations, num 1 (2010).

Also negative consequences of “virtual communication” for the value orientations of a person and society, and as a result for information security, are:

- regular and prolonged consumption of a large amount of surrogate information or the so-called “information garbage” (information of dubious quality, violence and horror, commercial advertising, etc.);
- surrogate communication, refusal to communicate with loved ones for the sake of “artificial” relationships with virtual acquaintances;
- zombie-making, as a result of which Internet addiction develops[28].

Thus, there is an urgent need to disseminate and approve humanistic values among the users of the Internet by spreading educational, popular scientific, religious, literary, and moral content in forms that are acceptable and attractive for different groups of population. The listed activities will undoubtedly strengthen the value basis of a democratic state’s information security.

The next factor that negatively affects the axiosphere of information security is the attempt of certain subjects of the information space to put their own private interests above the national interests and their desire to use information technologies for manipulating the public consciousness.

In strategic aspect, democratic states should strengthen the society’s axiosphere by reproducing values through education and upbringing, taking care of information security and protecting the country’s cultural-informational field from external influences. The information stability and embodiment of clear value priorities for the democratic development of a state will ensure its competitiveness in modern globalization processes.

Scientists believe that the stability of a society’s information field involves the development and approval of a sustainable system of democratically-oriented priority values. It is necessary to define the basic values that serve as a basis for grouping other values and ideas and creating safe conditions for the existence of an individual and the society as a whole. The system of democratic values is aimed at uniting communities and citizens and ensuring decent and safe living conditions in a modern society. According to experts, the analysis of the value priorities of personal security forms the basis for the formulation of a regulatory policy of the Ukrainian society’s value system, primarily through political actions of citizens and social groups[29].

According to the authors of this research, the understanding of information security should include not only the protection of the information resources of the society, state and people, but also the preservation of the value aspects of historical memory, cultural traditions, and a particular people’s specific national way of life. In this regard, researchers note the protection of a country’s information sovereignty, which implies legal, political, value and cultural, as well as information processes in the state. It is quite logical that information security programs are first of all aimed at protecting the state’s sovereignty.

[28] K. Kerdellan y H. Hrezyion, Dety protsessora: Kak Ynternet y vydeoyhrы formyruiut zavtrashnykh vzroslыkh: [Per. s fr] (Ekaterinburg: U-Factor, 2006).

[29] I. O. Bushman, “Tsinnisni oriientyry suchasnoho suspilstva. Hileia: naukovyi visnyk”,  Gilea: Scientific Bulletin, issue 102 (2015).

A. Oliynyk points out that the information security system directly affects the provision of information sovereignty and is an appropriate set of mechanisms for implementing the constitutional principles of Ukraine’s sovereignty and independence. Information sovereignty is an important condition for ensuring information security, i.e. information sovereignty and information security are interrelated[30].

Expanding the hypothesis of their research, the authors note that the protection of the country’s information sovereignty and the provision of an individual’s information security should concern state bodies, private structures and subjects of civil society. In a democratic society, the latter actively participate in the formation and popularization of various values that form the basis for the formation of the institute of information security.

Practice shows that individual private companies – even those with powerful resources – cannot fully and effectively counteract cybercrime. Therefore, there is a need for fruitful cooperation between commercial and governmental structures to protect common information interests.

Proceeding from the foregoing, the increase in the computer literacy level of employees of both state and commercial structures acquires special importance. In this regard, M. Hickman emphasizes the importance of training. Although many IT managers believe that everything is alright, it is critical to consider whether employees are able to act in abnormal situations in addition to acting according to established rules. After all, all firewalls in the world cannot fully resist human error or criminal human intentions, which can cause significant harm and lead to information loss, for example, because of fishing attacks or malicious software[31]. Thus, experts believe that it is necessary to have effective models of information systems that allow programmers and system administrators to successfully predict the risk of threats, plan and implement security measures, allocate corresponding resources and, accordingly, protect information systems[32].

Accordingly, the competence of those working with information, as well as awareness of the methods of its storage and protection are an immutable value of a modern democratic state. That is why computer, information and communication literacy is the most important condition for ensuring the information security of all subjects involved in social relations. According to scientists, in recent years there has been a sharp increase in the activity of various types of organized criminal groups, as well as extremist and terrorist organizations that interfere in the information space to achieve their own dishonest goals. This includes crimes in various spheres of administration and management, hacking attacks on government websites and portals, as well as bank databases, and attempts to destabilize the activities of critical infrastructure facilities and the socio-political situation in a certain region or a state as a whole, etc. Cyber espionage keeps becoming more widespread[33].

[30] O. Oliynyk, “Informatsiynyy suverenitet yak vazhlyva umova zabezpechennya informatsiynoyi bezpeky Ukrayiny. Naukovi zapysky Instytutu zakonodavstva Verkhovnoyi Rady Ukrayiny”, Scientific notes the Institute of Legislation Verkhovna Rada of Ukraine, num 1 (2015).

[31] M. Hickman, “The threat from inside”, Network Security, num 4 (2017).

[32] S. Rajasooriya; C. Tsokos y P. Kaluarachchi “Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability”, Journal of Information Security, num 8 (2017).

[33] O. F. Hida, “Mizhnarodni initsiatyvy u sferi posylennia informatsiinoi bezpeky ta protydii orhanizovanii zlochynnosti. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)”, The Fight Against Organized Crime and Corruption (theory and practice), issue 1 (2012).

As it is known, cybercrime is destructive to the axiological basis of the state's and society's information security and violates such basic values as fairness in the use of information resources, equality in access to information databases, legal protection of individual and authorial information, substitution of legal freedom with anarchy in the information space, etc.

Cybersecurity has become a major issue of concern in most areas of human life that are directly or indirectly related to cyber-physical systems. For example, industrial network systems used for automated production facilities and control processes have now become subject to the same threats and attacks of hackers as ordinary users do every day[34].

Users of personal computers are especially unprotected and vulnerable to information threats since people who often have very little awareness of technologies and insufficient understanding of the consequences of their use have to decide independently how to protect themselves[35].

Thus, various manifestations of cyberterrorism are a potential threat that can undermine the foundations of national security aiming at the most important elements of the infrastructure. This threat is most evident in developed societies given the increasing role of technologies in most spheres of life[36].

Despite the importance of technological aspects in the information security system, it is possible to state that the value component is an indispensable element of various framework and normative documents that regulate the activity of entities in the information sphere and protect it from cybercrime. The major Foreign Policy Initiative of the United States about the perspectives for the development of cyberspace, which was promulgated on May 16, 2011 under the name of International Strategy for Cyberspace, contains a number of "basic principles" that reflect the value-ideological orientation of the document. According to this Strategy, such basic principles include:

− "fundamental freedoms" (to right to seek, receive, and impart information and ideas through any media and regardless of frontiers);

− "privacy" (people should be aware of the threats of their personal information and the possibility of cybercrime against them);

− "free information flows" (the flow of information should not be limited to filters and firewalls as they create seeming security. Cyberspace should be a place for innovation and cooperation between the state and business for greater security)[37].

At the same time, the information society predetermines and produces a more complex, reflective understanding of freedom – "paradoxical freedom". Its essential characteristics are the inevitable assumption of responsibility for the obvious and latent consequences of risks: the social subject is placed in such conditions when it is necessary

[34] M. Cheminod; L. Durante; L. Seno y A. Valenzano, "Detection of attacks based on known vulnerabilities in industrial networked systems", Journal of information security and application, num 34 (2017).

[35] N. Thompson; T. McGill y X. Wang, ""Security begins at home": Determinants of home computer and mobile device security behavior", Computers & Security, num 70 (2017).

[36] A. Alqahtani, "Awareness of the Potential Threat of Cyberterrorism to the National Security", Journal of Information Security, num 5 (2014).

[37] D. V. Dubov y M. A. Ozhevan, Maibutnie kiberprostoru ta natsionalni interesy Ukrainy: novi mizhnarodni initsiatyvy providnykh heopolitychnykh hravtsiv : analit. dop. (Kyiv: NISD, 2012).

to constantly choose. Evaluation of the choice made actively vary in the sociocultural space and change over time. A choice that is functional, effective for one cultural space is not universal for other cultures. Deviation in one value-normative space becomes an innovation in another. The “freedom of risk” is becoming a norm of security ensuring practices[38].

It is quite obvious that the expansion of the boundaries of freedom in the information space created the ground not only for self-realization of a person and the progress of society, but also increased the palette of risks for the functioning of a modern state. As L. Svendsen notes, the circumstances of personal freedom have changed dramatically. Normal living standards, an excess of time and material resources in modern conditions have become available not only to a few minorities, which has turned the freedom of choice into one of the central concepts of human existence[39]. It can be stated that in a modern democratic, information society, all subjects received more freedom (in comparison with other types of societies), while taking responsibility for the choice made and possible risks.

That's why, strengthening of the axiological component of a state’s information security and legislative consolidation of values is the most important step in the protection of a country’s spiritual sphere and information sovereignty.

As noted above, civil society actors, namely analytical and scientific centers, public organizations and movements, law-abiding users of social networks play an important role in ensuring the information security of a state and the reproduction of its value component.

In this regard, Yu. Lisovs’ka notes, that the inclusion of civil society institutions in the information security system gives a solution to a number of relevant problems. First of all, it ensures public participation in making decisions about information security issues. Secondly, the introduction of civil society institutions in the mechanism of the information security policy ensures the process of involving citizens in solving information security problems and their active position on relevant issues[40].

In this context, scientists argue that the social network does not have a single institutionally fixed control center, and therefore it is almost impossible to destroy it, as long as modern society exists. Almost invulnerable are also the various criminal and terrorist networks against which state structures are fighting. A certain role in the fight against criminal networks, helping law enforcement agencies, primarily with the information, can be carried out by the subjects of social networks that are law-abiding, aware of their constitutional rights and obligations[41].

Of course, in order to overcome the negative manifestations of information freedom and suppress the activities of criminal network structures, a democratic state must rely on

[38] A. Getman; O. Danilyan; A. Dzeban; Y. Kalinovsky y Y. Hetman, “Information security in modern society: sociocultural aspects”,Amazonia Investiga vol: 9 num 25 (2020).

[39] L. Fr. H. Svendsen, Filosofiia svobody / per. z norvezk (Lviv: Vydavnytstvo Anetty Antonenko; Kyiv: Nika-Tsentr, 2016).

[40] Yu. P. Lisovs'ka, “Administratyvno-pravova diyal'nist' nederzhavnykh orhaniv ta orhanizatsiy yak strukturnykh elementiv systemy zabezpechennya informatsiynoyi bezpeky. Naukovi pratsi MAUP”, Scientific works IAPM, issue 2 (2014).

[41] Ya. V. Liubyvyi, “Sotsialna refleksiia yak mekhanizm samoorhanizatsii sotsialnykh merezh. Multyversum. Filosofskyi almanakh”, Multiversum. Philosophical Almanac, issue 1-2 (2016).

law-abiding citizens, self-organizing structures of civil society, which today are widely represented on the Internet. The importance of attracting civil society institutions to strengthen the state's information security is determined, according to experts, by the expansion of the range of information dissemination entities whose activities are not always fully regulated by law, but which can be influenced by other entities of the virtual space with high moral and civil qualities, creating in the network the atmosphere of rejection of extremism, explaining to less prepared citizens the essence of manipulative technologies, warning the law-enforcement agencies about the illegal actions and intentions of individuals and organizations.

By involving citizens in information security activities, public organizations perform axiological, instructive and educational functions by forming public opinion on important issues of protecting the information interests of the state and citizens.

Modern democratic countries demonstrate a stable practice of cooperation between state and non-state entities of information security, which found a reflection at the legislative level as well and contributed to the legal consolidation of various values. For example, on November 26, 2003, the US Congress introduced the Home Security Act. Accordingly, the Department of Homeland Security, which is responsible for coordinating the activities of state bodies and all private entities on information security issues, was established. This law provides for the development of the National Strategy to Secure Cyberspace and the National Strategy for the Physical Protection of Critical Infrastructures. The listed documents provide for the formation of a unified national system for countering cyberterrorism. Within the framework of this system, the creation of territorial, departmental and private centers of counteraction was initiated, and their functions and interaction procedure were determined[42].

European states are also moving in a similar direction. In February 2011, the Government of the Netherlands adopted the National Cybersecurity Strategy named "Strength through Cooperation", which provides for the formation of the National Council for Cybersecurity. The goal of this entity is to ensure the implementation of an approach based on cooperation between the public and private sectors, and scientific centers. In addition, it is planned to establish a National Center for Cybersecurity, which should be aimed at identifying trends and threats to information security, as well as contributing to the elimination of the consequences of incidents and crisis situations in this field[43].

The analysis of the regulatory and legal framework of the above democratic states, which regulates the participation of non-state entities as structural elements of the information security system, makes is possible to single out the following basic forms: participation in the work of consultative and advisory bodies in the field of public administration in the information sphere; participation in public social discussions held by the government in the information sphere; participation in the examination of public opinion conducted by the government in the information sphere; sending inquiries and complaints to public authorities in the information sphere in the course of public control over

[42] R. V. Aliamkin y M. P. Fedorin, "Pravove zabezpechennia natsionalnoi informatsiinoi bezpeky. Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy", Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine, num 4 (2013).

[43] Report of the Governmental Experts Group on Advances in the Area of Information and Telecommunications in the Context of International Security (A/65/201) (New York, United Nations, 2012).

compliance with the law, and sending applications (petitions) about the satisfaction of rights and legitimate interests in the information sphere to public administration bodies[44].

Also, to ensure the appropriate level of information security of the state, it is necessary to clearly understand the functions and features of the activities of subjects of the Internet space, improve the legislation governing the extent of their influence on public relations. From the point of view of D. Protsenko, the above entities can be grouped depending on their functions, rights and obligations as follows:

1) Internet providers are pure technical intermediaries, since they only deal with telecommunication networks, hardware and their smooth operation for the needs of users;
2) owners of websites that have full control over all materials posted on websites, that is, persons who exercise full editorial control;
3) owners of websites with the areas for free posting of information (forums, comments, etc.), that is, people who have limited or partial editorial control over the content of the site, which is manifested as follows: persons have full editorial control over editorial materials site, as well as limited editorial control over messages of unauthorized persons, carried out in the form of pre-moderation or post-moderation of such messages;
4) correspondent authors who leave messages in the areas where information is freely available on certain sites or are the authors of editorial materials, in this case, the relations with the editorial office must have civil law registration;
5) owners of the tools of personalization that are used on websites or other services, “with” or “without” editorial control rights;
6) domain name registrants whose data are contained in the registration database of various domains[45].

Thus, non-state subjects of information security have the opportunity to widely and publicly discuss political, legal, moral and other values, to assert their importance in public life, to make an influence on the formation of value grounds for public consciousness and, consequently, directly and indirectly participate in the protection of the state’s information sovereignty.

K. Zakharenko rightly asserts that non-state analytical centers are influential non-state subjects of a country’s information security. The role of non-governmental analytical centers as generators of new ideas and alternative approaches is especially important in transitional societies, where profound internal transformations are inherent in all spheres of social life, in particular, in the sphere of information security. In addition, non-governmental analytical centers are an instrument for public control. They influence the definition of the society’s goals and values and form public opinion, which is the main object of information attacks by other states[46].

Thus, analytical centers (both governmental and non-governmental) can significantly strengthen the value-cognitive basis of information security of a democratic state. As a

[44] Yu. P. Burylo, “Uchast nederzhavnykh subiektiv u zdiisnenni derzhavnoho upravlinnia informatsiinoiu sferoiu. Pravova informatyka”, Legal Informatics, num 4 (2007).

[45] D. V. Protsenko, “Zakhyst prava na svobodu vyrazhennia v merezhi Internet: mizhnarodni tendentsii ta ukrainski realii. Naukovi zapysky NaUKMA. Yurydychni nauky”, NaUKMA Research Papers. Law, Vol 144-145 (2013).

[46] K. Zakharenko, "Efektyvnist vykorystannia potentsialu nederzhavnykh subiektiv informatsiinoi bezpeky. Multyversum. Filosofskyi almanakh”, Multiversum. Philosophical Almanac, issue 1–2 (2016).

rule, they offer a scientifically grounded solution to complex problems in this sphere, as well as provide intellectual support to various actors in the information field. Unfortunately, the opportunities provided by these structures are not always rationally used by state bodies that are responsible for information security; in particular, their analytical developments are not practically implemented.

The analysis of the points of view presented in this paper and the author's vision of the problem allow us to further focus on more detailed developments of the institutional and non-institutional aspects of ensuring information security in its axiological dimension.

## Conclusions

The creation of a democratic state's information security system requires an integrated approach that incorporates a number of aspects - economic, political, technical, technological, spiritual, cultural, legal, etc. In modern conditions of global competition based on knowledge and technology, the information security problem has undergone significant transformations.

Of course, values are the most important component of the information security of the state, society and a man, since information attacks are aimed primarily at the cognitive-spiritual structures of social and individual consciousness. The protection of the system-forming values of a democratic state requires constant efforts on the part of both power institutions and civil society actors. As it is known, the basic values of democratic development are freedom, legal equality, social justice, security, human rights, etc. The analysis carried out in this work shows that democratic countries are in a constant search for a compromise between the restrictive measures introduced to ensure national security and the full realization of human rights and freedoms, including in the information sphere. Reflecting on the ranking of values in democratic countries, we can state that the basic of them is freedom in its various manifestations.

At present, it can be stated that the legislative framework of a number of democratic countries, regulating the activities of entities in the information space, is imperfect and does not preclude the possibility of unlawful actions against the information security of the state. This study demonstrates that government agencies need to more dynamically and effectively establish cooperation with civil society in ensuring the spiritual and value component of information security, and constantly improve legislation in the information sphere. Through educational and enlightening programs, it is necessary to systematically clarify the importance of democratic values, show the ways of their legal protection, and also emphasize in every way the relationship between the values of public consciousness and progress.

## References

Aliamkin, R. V. y Fedorin, M. P. "Pravove zabezpechennia natsionalnoi informatsiinoi bezpeky. Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy". Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine, num 4 (2013): 91-96.

Alqahtani, A. "Awareness of the Potential Threat of Cyberterrorism to the National Security". Journal of Information Security, num 5 (2014): 137-146.

Belanger, F.; Collignon, St.; Enget, K. y Negangard, E. "Determinants of early conformance with information security policies. Information and Management", num 54 (2017): 887-901.

Burylo, Yu. P. "Uchast nederzhavnykh subiektiv u zdiisnenni derzhavnoho upravlinnia informatsiinoiu sferoiu. Pravova informatyka". Legal Informatics, num 4 (2007): 31−41.

Bushman, I. O. "Tsinnisni oriientyry suchasnoho suspilstva. Hileia: naukovyi visnyk". Gilea: Scientific Bulletin, issue num 102 (2015): 201-205 [in Ukrainian].

Cheminod, M.; Durante, L.; Seno, L. y Valenzano, A. "Detection of attacks based on known vulnerabilities in industrial networked systems". Journal of information security and application, num 34 (2017): 153-165.

Chichanovskyi, A. A. y Starish, O. H. Informatsiini protsesy v strukturi svitovykh komunikatsiinykh system. Kyiv: Hramota. 2010.

Dmyterko, Yu. Yu. "Vidobrazhennia diisnosti u ZMI: derzhavno-pravovyi aspekt zhurnalistyky. Efektyvnist derzhavnoho upravlinnia". Efficiency of Public Administration, issue 38 (2014): 361-367.

Dubov, D. V. y Ozhevan, M. A. Maibutnie kiberprostoru ta natsionalni interesy Ukrainy: novi mizhnarodni initsiatyvy providnykh heopolitychnykh hravtsiv: analit. dop. Kyiv: NISD. 2012.

Ewurah, S. K. "The Concept of Government: ICT Policy Guidelines for the Policy Makers of Ghana". Journal of Information Security, num 8 (2017): 106-124.

Getman, A.; Danilyan, O.; Dzeban, A.; Kalinovsky, Y. y Hetman, Y. "Information security in modern society: sociocultural aspects". Amazonia Investiga, Vol: 9 num 25 (2020): 6-14.

Gusmão, A.; Silva, L.; Silva, M.; Poleto, T. y Costa, A. "Information security risk analysis model using fuzzy decision theory". International Journal of Information Management, num 36 (2016): 25-34.

Hickman, M. "The threat from inside". Network Security, num 4 (2017): 18-19.

Hida, O. F. "Mizhnarodni initsiatyvy u sferi posylennia informatsiinoi bezpeky ta protydii orhanizovanii zlochynnosti. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)". The Fight Against Organized Crime and Corruption (Theory and Practice), issue 1 (2012): 258-266.

Islama, M.; Watsonb, J.; Iannella, R. y Geva, S. "A greater understanding of social networks privacy requirements: The user perspective". Journal of information security and application, num 33 (2017): 30-44.

Kerdellan, K. y Hrezyion, H. Dety protsessora: Kak Үnternet у vydeoуhrы formyruiut zavtrashnykh vzroslыkh: [Per. s fr]. Ekaterinburg: U-Factor. 2006.

Khimey, V. "Osnovni suchasni problemy informatsiynoyi bezpeky Ukrayiny. Tele- ta radiozhurnalistyka". Tele- and radio journalism, issue num 13 (2014): 127−132.

Ki-Aries, D. y Failyє, S. “Persona-Centred Information Security Awareness”. Computers & Security, num 70 (2017): 663-674.

Kokarcha, Yu. A. “Internet yak chynnyk politychnoi sotsializatsii osobystosti v suchasnomu suspilstvi. Naukovyi chasopys NPU imeni M. P. Drahomanova. Seriia 22: Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin”. Scientific Journal of National Pedagogical Dragomanov University. Series 22. Political Sciences and Methods of Teaching Socio-Political Disciplines, issue num 18 (2015): 80-86.

Kravchenko, T. O. “Aksiolohichnyi aspekt informatsiino-merezhevoi paradyhmy. Filosofiia nauky: tradytsii ta innovatsii”. Philosophy of Science: Traditions and Innovations, num 1 (2010): 53-63.

Lisovs'ka, Yu.P. “Administratyvno-pravova diyal'nist' nederzhavnykh orhaniv ta orhanizatsiy yak strukturnykh elementiv systemy zabezpechennya informatsiynoyi bezpeky. Naukovi pratsi MAUP”. Scientific works IAPM, issue 2 num 41 (2014) 108–113.

Liubyvyi, Ya. V. “Sotsialna refleksiia yak mekhanizm samoorhanizatsii sotsialnykh merezh. Multyversum. Filosofskyi almanakh”. Multiversum. Philosophical Almanac, issue num 1-2 (2016): 3-24.

Lysak, V. F. y Ahyeyeva, O. L. “Suchasni ukrayins'ki “mozkovi tsentry” yak sub"yekty suspil'no-politychnoho protsesu v derzhavi. Hileya: naukovyy visnyk”. Hilea: scientific journal, issue num 95 (2015): 377−382.

Oliynyk, O. “Informatsiynyy suverenitet yak vazhlyva umova zabezpechennya informatsiynoyi bezpeky Ukrayiny. Naukovi zapysky Instytutu zakonodavstva Verkhovnoyi Rady Ukrayiny”. Scientific notes the Institute of Legislation Verkhovna Rada of Ukraine, num 1 (2015): 54−59.

CUADERNOS DE SOFÍA
EDITORIAL

Las opiniones, análisis y conclusiones del autor son de su responsabilidad
y no necesariamente reflejan el pensamiento de **Revista Inclusiones**.