Information Security of a Modern Democratic State: Axiological Context

Seguridad de la información de un Estado democrático moderno: contexto axiológico

Oleg Gennadievich Danilyan[1]
Yaroslav the Wise National Law University - Russia
odana@i.ua

Aleksander Petrovich Dzeban[2]
Yaroslav the Wise National Law University - Russia
a_dzeban@ukr.net

Yury Yurievich Kalinovsky[2]
Yaroslav the Wise National Law University - Russia
kalina_uu@ukr.net

Inna Igorevna Kovalenko[3]
Yaroslav the Wise National Law University - Russia
kinna087@gmail.com

Julia Vasilyevna Melyakova[3]
Yaroslav the Wise National Law University - Russia
melyak77828@gmail.com

Vadim Olegovich Danilyan[4]
Yaroslav the Wise National Law University - Russia
danilyanvadim@rambler.ru

ABSTRACT

The authors of the research focus on the role and significance of values in forming the basis for the information security of a modern democratic state. In the course of the research, the authors applied general scientific methods (analysis, synthesis, analogy, etc.), philosophical methods (dialectical, hermeneutic), and special legal methods (normative-analytical). Information security includes not only the protection of information resources of the society, state and people, but also ensures the preservation of value aspects, historical memory, cultural traditions, and a particular people's specific national way of life. The most important objective of information society institutions is the protection of the country's information sovereignty. Information wars are the continuation of economic, political, as well as cultural and religious conflicts on our planet. In this research, the authors come to the conclusion that one of the aspects of information wars is value confrontation. That is why it is necessary to consider information security not only in the legal, communication-technical and political aspects but also in the axiological context.

Keywords: national security; information security; values; information sovereignty; information war.

RESUMEN

Los autores de la investigación se centran en el papel y la importancia de los valores para formar la base de la seguridad de la información de un estado democrático moderno. En el curso de la investigación, los autores aplicaron métodos científicos generales (análisis, síntesis, analogía, etc.), métodos filosóficos (dialécticos, hermenéuticos) y métodos legales especiales (normativo-analíticos). La seguridad de la información incluye no solo la protección de los recursos de información de la sociedad, el estado y las personas, sino que también garantiza la preservación de los aspectos de valor, la memoria histórica, las tradiciones culturales y la forma de vida nacional específica de un pueblo en particular. El objetivo más importante de las instituciones de la sociedad de la información es la protección de la soberanía de la información del país. Las guerras de información son la continuación de conflictos económicos, políticos, culturales y religiosos en nuestro planeta. En esta investigación, los autores llegan a la conclusión de que uno de los aspectos de las guerras de información es la confrontación de valores. Es por eso que es necesario considerar la seguridad de la información no solo en los aspectos legales, de comunicación, técnicos y políticos, sino también en el contexto axiológico.

Palabras clave: seguridad nacional; seguridad de información; valores; soberanía de la información; guerra de información

1Corresponding author. Dr. habil. in Philosophy, Professor Head of the Chair of Philosophy, Yaroslav the Wise National Law University
2Dr. habil. in Philosophy, Professor Chair of Philosophy, Yaroslav the Wise National Law University
3 Dr. habil. in Philosophy, Associate Professor Chair of Philosophy, Yaroslav the Wise National Law University
4 Dr. habil. in Philosophy, Associate Professor Chair of Philosophy and Sociology, Yaroslav the Wise National Law University

Recibido: 08/09/2019 Aceptado: 06/11/2019

Introduction

In the conditions of wide dissemination of information wars at the local and global levels, the importance of strengthening the information security of a democratic state is beyond doubt. Information security has several basic dimensions, the axiological one being the most important one. The formation and development of the value basis for the information security of a democratic state is a required condition for resisting information aggression, preserving the national identity, as well as the cultural and information sphere of a particular country.

The importance of the axiological determinants of a democratic state's information security is, first of all, conditioned by the fact that one of the forms of information aggression is the active influence on the values of social and individual consciousness, namely the destruction, substitution, and deformation of values.

This research is aimed at comprehensively analyzing the role and place of values in the system of ensuring the information security of a democratic state, generalizing domestic and foreign experience in this field, studying the communication-technical, legal and other aspects of preserving the value potential of a democratic state.

The working hypothesis of this research is based on the fact that the phenomenon of information security incorporates cultural, national, legal, political, religious and other values that constitute the basis for the public consciousness of a particular people. In a democratic society, where value pluralism prevails, it is especially important to protect freedom on the one hand and to prevent the erosion of the existing moral, religious and cultural grounds on the other hand. According to the analysis of scientific literature on this issue, the consideration of the phenomenon of information security in the context of values was carried out fragmentarily and did not have a complex nature.

The Problem of Information Security in Modern Scientific Literature

In scientific literature, the problems of information security were touched upon from various methodological positions, which helped to reveal the numerous aspects of this phenomenon, including the legal, economic, political, technical, communication, as well as spiritual and value related aspects. In particular, the researchers O. Radchenko and O. Bukhtaty (2014) distinguish three aspects of modern information and communication relations: ideological, information, and technological, which make the basis for modelling the modern state communication policy (Radchenko, Bukhtaty, 2014, p. 82).

M. Zaytsev (2013), in his turn, examines the phenomenon of information security in the context of a unified national security system of a state and emphasizes the need to protect the information interests of citizens, the society and the sate.

In his research, T. Kravchenko (2014) analyzes the activity of networked communities in the context of values and highlights the positive and negative aspects of their influence on the information security of a state. According to Y. Dmyterko (2014), the legislatively unsettled communication and information relations have a negative impact on the information security of all actors involved in the process of ensuring information security. The negative impact is related to the gaps in legislation and the ambiguity of interpreting certain norms.

I. Bushman (2015) focuses on the need to develop and support the basic values of a democratic state's social development. Value consensus is the most important basis for the information security of a democratic political system. A. Oleinik (2015) substantiates the dialectical relationship of a state's information sovereignty to the information security system and reveals their interdependence and mutual influence.

Civil society institutions play an important role in ensuring the information security of a democratic state and its value component. Y. Liskovskaya interprets this idea in her scientific study, "Administrative and Legal Activities of Non-State Bodies and Organizations as Elements of the Information Security System" (2014). A. Golovka (2016) adheres to similar ideas and views the importance of civil society institutions in the context of ensuring the information security of the Ukrainian State. In his turn, Zakharenko (2016) argues that non-governmental analytical centers that develop and relay socially significant concepts, ideas, and values are the most influential non-state actors in the state's information security. At the same time, researchers V. Lysak and O. Ageyeva (2015) emphasize that the problem in the activity of analytical centers as subjects of information security is related to the unwillingness of state authorities to cooperate with external sources of information and different projects, which entails secrecy and non-transparency in the process of preparing and making decisions by the state's highest political leaders (Lysak, Ageyeva, 2015 p. 380).

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 (2014) argues that they are caused by deformations of the information space under the influence of various objective and subjective factors. 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 (Ewurah, 2017, p. 109-110).

According to S. Qadir and S. Quadri (2016), when ensuring information security the parties concerned should maintain the functioning of three main 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 (Qadir, Quadri, 2016, p. 192).

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. Islam, J. Watsonb, R. Iannella and S. Gueva (2017) 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. 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.

Expanding the above hypotheses, A. Veiga and N. Martins (2017) 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.

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 (Safa, Maple, 2017, p. 17). 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 (Safa, Solms, Futcher, 2016). 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 (Safa, Solms, 2016). 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, antiphishing, antispyware, firewalls, authentication and intrusion detection systems constitute the technological aspect aimed at information protection. However, they cannot guarantee a safe environment for information (Safa, Solms, Furnell, 2016.

F. Belanger, C. Collignon, K. Enget, E. Negangard (2017) come to the conclusion that information is one of the most valuable assets of 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 (p. 889).

It is quite obvious that the value-related aspect of information security directly correlates with the cognitive, communication and technical aspects of this phenomenon. The protection of the values and rights of people, the society and the state in the information sphere is a relevant problem for modern democratic states.

Thus, the analysis of the scientific literature on the problem of information security in the context of values gives grounds to assert that the studies conducted are fragmentary and there is a need to generalize and expand the existing viewpoints.

The Human Right to Information and Information Security

In the conditions of modern global processes, information is a powerful resource that promotes national progress. That is why the availability of high-quality (reliable) information, its storage, protection and processing speed constitute the required prerequisites for the stable existence of the state. At the same time, the realization of the human right to reliable information is a necessary component of a society's democratic development.

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 his 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 (Радченко, Бухтатий, 2014, p. 82).

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 (Pernebekova, Beisenkulov, 2015, p. 271).

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-Owen and S. Faily 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 (Ki-Aries, Failyє, 2017, p. 664).

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 threats to information systems and the dangers of implementing countermeasures that reduce risks to an acceptable level (Gusmão et al., 2016, p. 25).

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 (Чічановський, Старіш, 2010, p. 390).

Value Basis of Information Security

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. Zyazyun 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 (Зязюн, 2010, p.11).

Analyzing the viewpoints of I. Zyazyun, 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 (Кравченко, 2014, p. 57).

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 the 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 the 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 (Бушман, 2015, p. 203).

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.

A. Oleynik 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 (Олійник, 2015, p. 58).

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 phishing attacks or malicious software) (Hickman, 2017, p. 15).

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 (Rajasooriya, Tsokos, Kaluarachchi, 2017, p. 126).

Competence in 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.

Cybercrime and Cyber Security Issues

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 (Гіда, 2012, p. 260).

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 (Cheminod et al., 2017, p. 153).

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 (Thompson et al., 2017, p. 390).

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 (Alqahtani, 2014, p. 145).

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) (Дубов, Ожеван, 2012, p. 4-5).

According to the authors of this research, 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, play an important role in ensuring the information security of a state and the reproduction of its value component.

In this regard, Y. Liskovskaya argues 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 (Лісовська, 2014, p. 110).

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 (Алямкін, Федорін, 2013, p. 93-94).

European states are also moving in a similar direction. In February 2011, the Government of the Netherlands adopted the National Cybersecurty 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 (UN, 2012, p. 30-31).

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 administrative 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 compliance with the law, and sending applications (petitions) about the satisfaction of rights and legitimate interests in the information sphere to public administration bodies (Бурило, 2007, p. 34).

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 (Захаренко, 2016, p. 59-60).

Thus, analytical centers (both governmental and non-governmental) can significantly strengthen the value-cognitive basis of information security of a democratic state. As a 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 above viewpoints on the problem of information security in the context of values helped clarify the authors' hypothesis, as well as its concretization in the legal and communication-information aspects.

Conclusion

Summarizing the foregoing, it is necessary to point out that a number of problems related to the information security of democratic states in its axiological dimension are due to deformations of the information space under the influence of various objective and subjective factors.

In a generalized form, the quintessence of mental, civilizational, political, legal, cultural and historical values and traditions that must ensure the stability of social development and the preservation of the national and cultural identity of a particular people constitute the axiological foundation of a democratic state's information security. An important component of protecting the information sovereignty of a democratic state is the re-creation of universal and national values both by state institutions and civil society actors. The state should stimulate the civil initiative to strengthen information security and create appropriate legal and economic conditions for the activities of civil society actors in this field.

In the conditions of global competition, information wars, cyberterrorism, cyber espionage, and information attacks on various communication and information systems have become widespread phenomena. In fact, information wars are a logical continuation of economic, political and cultural-religious conflicts on our planet. The authors of this research come to the conclusion that value confrontation is one of the aspects of information wars. Therefore, there is a need to consider information security not only in the legal, communication-technical and political aspects but also in the axiological context. Protecting their own cultural and information space, democratic states protect a number of important values, namely human rights, freedom, equality, security, nomocracy, and justice.

The results of this research can be used in further research in the field of information security in the anthropological, ontological and value-related dimensions. The research enhances the scientific and methodological potential for understanding the essence and trends in the field of information security in the modern world. From the practical point of view, the results of the research can serve as a basis for modernizing the existing approaches and concepts in the field of information security of democratic states and a theoretical basis for the preparation of law acts and by-laws in this field. The research foregrounds the problem of interaction between the state and civil society institutions in the process of ensuring the information sovereignty of a country, which, in turn, requires the introduction of integrated programs of interaction and reinforcement of their practical orientation.

In further studies on the problem of information security in the axiological context, it is necessary to focus on the consideration of various aspects of values and their correlation in the activity of modern democratic states. Thus, it is necessary to analyze the correlation of such value determinants of an information society as freedom and responsibility, equality and justice, security and human rights. The problem of the protection of the human right to information and its legislative consolidation requires a comprehensive consideration. The study of new norms, methods, and manifestations of information wars, cyberterrorism and cyber espionage is the most important direction for scientific and applied research in this field.

BIBLIORAPHIC REFERENCES

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

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

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

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

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

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

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

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

Pernebekova, A., Beisenkulov, A. (2015). Information Security and the Theory of Unfaithful Information. *Journal of Information Security,* 6: 265-272.

Qadir, S., Quadri, S. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security,* 7: 185-194.

Rajasooriya, S., Tsokos, C., Kaluarachchi, P. (2017). Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability. *Journal of Information Security,* 8: 125-140.

Safa, N., Maple, C. (2016). Human errors in the information security realm – and how to fix them. *Computer fraud and security,* 9: 17-20.

Safa, N., Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57: 442-451.

Safa, N., Solms, R., Furnell, St. (2016). Information security policy compliance model in organizations. *Computers & Security,* 56: 70-82.

Safa, N., Solms, R., Futcher, L. (2016). Human aspects of information security in organisations. *Computer fraud and security*, 2: 15-18.

Thompson, N., McGill, T., Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70: 376-391.

Veiga, A., Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70: 72-94.