Information security in modern society: Sociocultural aspects

Інформаційна безпека у сучасному суспільстві: соціокультурні аспекти розуміння

Written by:
Getman Anatolii P.[1]
ORCID ID: 0000-0002-1987-2760
Danilyan Oleg G.[2]
ORCID ID: 0000-0001-5308-4664
Dzeban Alexander P.[3]
ORCID ID: 0000-0002-2075-7508
Kalinovsky Yury Y.[4]
ORCID ID: 0000-0002-0081-8107
Hetman Yevhen A.[5]
ORCID ID: 0000-0002-1801-7252

Abstract

The purpose of the work is to study the major conceptual socio-cultural features of the essence and ensuring the information security in an information society. The research methodology is based on a complex combination of philosophical (dialectical, hermeneutical) and scientific methods to study the problem of security in modern society, and especially empirical, comparative, analytical and descriptive. They are based on the principles of consistency and historicity that allows exploring contemporary socio-cultural processes and phenomena in the dynamics and in connection with the historical conditions of their development as well as with the security issues. The scientific novelty of the work is in revealing key aspects of understanding the essence and ensuring the information security, in defining the most significant features in conditions of the the information society. Conclusions. Ensuring the information security in modern society depends on many factors, including how a person will behave in this or that stressful situation. The key risks factors for the information subsystem of the society are large-scale socio-communicative and socio-cultural transformations, which carry a number of negative social consequences. In recent years, disorganizing and dysfunctional trends, directly

Анотація

Мета роботи − дослідити основні концептуальні соціокультурні особливості сутності й забезпечення інформаційної безпеки в інформаційному суспільстві. Методологія дослідження ґрунтується на комплексному поєднанні філософських (діалектичний, герменевтичний) та загальнонаукових методів дослідження проблеми безпеки у сучасному суспільстві, зокрема емпіричному, компаративістському, аналітичному та дескриптивному. Вони базуються на принципах системності та історичності, що дозволяє вивчати сучасні соціокультурні процеси та явища у динаміці та у зв'язку як з історичними умовами їх розвитку, так і з безпековою проблематикою. Наукова новизна роботи полягає у розкритті ключових аспектів розуміння сутності й забезпечення інформаційної безпеки, визначенні найбільш істотних її особливостей в умовах інформаційного суспільства. Висновки. Забезпечення інформаційної безпеки у сучасному суспільстві залежить від багатьох факторів, у тому числі й від того, як буде вести себе людина в тій чи іншій стресовій ситуації. Ключовим фактором ризику для інформаційної підсистеми соціуму

[1] Doctor of Legal Sciences, Professor, Pro-Rector for Scientific Work, Yaroslav Mudryi National Law University.
[2] Doctor of Philosophical Sciences, Professor, Head of the Department of Philosophy at Yaroslav Mudryi National Law University
[3] Doctor of Philosophical Sciences, Professor, Professor of the Department of Philosophy at Yaroslav Mudryi National Law University
[4] Doctor of Philosophical Sciences, Professor, Professor of the Department of Philosophy at Yaroslav Mudryi National Law University
[5] Doctor of Legal Sciences, Professor, Senior Research Fellow, Head of Department of Coordination of Legal Studies of National Academy of Legal Sciences of Ukraine

related to the high speed of information change are clearly recorded. The traditional practice of information security and security against the information become more complex due to the development of virtual social reality of cyberspace. Modern communication processes lead to the information redundancy and enhance the "fissure" between the virtual and real worlds, which affects the growth of the conventions of network practices of the information security. The overabundance of low quality information, which is observed at this stage of development of the information society is not the only problem of the information security. The problem of forming the appropriate level of information culture that would prevent the emergence of her stressful situations when working with information and information technology is also among such issues. Information security in the information society is the protection of information and protection against the information. Ensuring the information security is a necessity, which becomes an attribute of modern life of any social entity, and requires a tireless work with the information that involves interaction with a variety of expert systems, the delocalization of actions, ensuring freedom and minimizing risks.

Key words: Information, information threats, information security, information technology, media, network practices.

виступають масштабні соціокомунікативні та соціокультурні трансформації, що несуть у собі низку негативних соціальних наслідків. В останні роки чітко фіксуються дезорганізаційно-дисфункційні тенденції, безпосередньо пов'язані з високими швидкостями інформаційних змін. Традиційні практики захисту інформації і від інформації ускладнюються через розвиток віртуальної соціальної реальності кіберпростору. Сучасні комунікаційні процеси ведуть до інформаційної надмірності й посилення «розлому» між віртуальним і реальним світами, що позначається на зростанні умовності мережевих практик інформаційної безпеки. Надлишок низькоякісної інформації, який спостерігається на даному етапі розвитку інформаційного суспільства є не єдиною проблемою забезпечення інформаційної безпеки. У дану проблематику також входить проблема формування у людини відповідного рівня інформаційної культури, який перешкоджав би виникненню у неї стресових ситуацій при роботі з інформацією та інформаційними технологіями. Інформаційна безпека в умовах інформаційного суспільства – це і захист інформації, і захист від інформації. Забезпечення інформаційної безпеки – це необхідність, яка стає атрибутом сучасного життя будь-якого соціального суб'єкта, і вимагає невпинної роботи з інформацією, що включає в себе взаємодію з різними експертними системами, делокалізацію дій, забезпечення свободи та мінімізації ризиків.

Ключові слова: інформація, інформаційні загрози, інформаційна безпека, інформаційні технології, інформаційна сфера, мережеві практики.

Introduction

Relevance of the research. Modern society is characterized by an unprecedented increase in the influence of the information component on social life, whatever conceptual characteristics we would give it - post-industrial, informational, market, civic and so on. By making normative definitions of reality, forming needs, views, assessments and preferences, information activity is one of the constitutive components of social reality. The emergence of new information technologies lays a solid foundation for the development of the global information community. In developed countries, this transition will lead to a change in social and economic relations. The contradictions of the integration strategies of globalization and regionalization are creating new information and virtual flows that produce information violence. At the present stage of human development, the social subject has entered a new phase, where the main subject of work is information and knowledge, the tools of work are information technology and communication media, and the society itself is gradually becoming information. Knowledge and information have become essential resources which allow to achieve the desired goals. In addition, the issue of information security, which occupies one of the

key places in the system of ensuring the vital interests of all countries without exception, is particularly relevant. This is primarily due to the urgent need to create a developed information environment of society as it is through the information environment the threats to national security in various spheres of activity of the individual, society and the state are more often realized.

Methodology

The full range of philosophical, general scientific and specific methods of scientific research intrinsic to philosophy are applied in this article in their interconnection and complementarity. The methodological basis for the study consists of the general scientific methods of information processes cognition in modern society, in particular empirical, analytical, comparative and descriptive methods. They are built on the principles of consistency and historicity, so it allows to study current processes and phenomena, that take place in the information sphere, in the dynamics and in the connection with the historical conditions of their development as well as with security issues. Furthermore, research methods are based on the principles of systematic and structural-functional analysis, which detect the level of information stability of the society and of the state.

Analysis of research and publications

Despite the sufficiently significant study of the problem of information security in its various manifestations, there is no unity in understanding the essence of this phenomenon in the current scientific paradigm. Unfortunately, the general philosophical understanding of this problem in the context of the information culture is also not at a proper level.

At the same time, in modern publications there are quite interesting separate points of view on the problem of information security in the conditions of avalanche-like development and introduction of information technologies into all spheres of society. For example, L. Khizhnyak rightly states that in conditions of sharp disbalance of positive and negative messages in the selection of materials, lack of correct discussion of different points of view, it becomes necessary to protect both the society and the individual from destructive information influences at the very stages of design, distribution and support a conventional unit of information and psychological influence which is a meme [Khyzhniak, 2017].

O.Markozova believes that "the information society and its system of values is not only a good that promotes the development of an independent personality, the development of his or her internal resources, but also threatens traditional values and culture, and modern civilization is rapidly transforming into "a society of risks", which complicates the processes of human activity " [Markozova, 2016].

In the context of the studied problem, C.Crabtree and M.Nelson's point of view, who define the ensuring the protection of human rights and freedoms in the information sphere, and the human being as the main its object, as one of the most important goals of information security, this point of view seems to be quite right [Crabtree & Nelson, 2017].

In the present day literature there are also scientific publications concerning the practical aspects of the problem of ensuring information security from the point of socio-humanitarian positions. Thus, for example, S.Ewurah, analyzing the state and prospects of deploying security processes, makes a well-backgrounded proposal that the main attention should be paid to the implementing web-portals, creating standards to maintain the functional interoperability of computer systems, providing a high-speed network for data exchange, improving the training of public officials engaged in information and communication technologies and improving the security of government databases [Ewurah, 2017].

In turn, S.Qadir and S.Quadri state that, while providing information security, interested parties need to support the functioning of three key attributes: confidentiality, integrity and accessibility. Accessibility is more critical of these attributes, since the other two depend on it directly, since it is impossible to use confidentiality and integrity methods without available information [Qadir & Quadri, 2016].

Similar views on the problem of information security are demonstrated by the researchers M. Islama, J. Watson, R. Iannella, S. Geva, emphasizing that confidentiality is not just a concealment of information, it is also a legitimate control over one's own personal information [Islama, Watson, Iannella & Geva, 2017]. In their view, the value of protecting one's own personal space as a condition of ensuring information security for a citizen is the most important factor in the development of a modern democratic state.

Developing the above points of view of A. Veiga and N. Martins note, that the leaders of different communities can influence the culture of citizens by using different approaches to creating an environment in which the information is protected. Successful management of information security depends on the authority of a leader, effective management practices in this field [Veiga & Martins, 2017].

According to N.Safa and C.Maple, information (computer) literacy is a key element of ensuring the information security. In their belief, to increase users' level of awareness the quality training in information security is needed. Using official presentations, games, websites, e-mails, meetings, etc. for this purpose have shown that they are the key methods for raising public awareness. Therefore, a high level of knowledge in the information and communication sphere allows all subjects of information security to become more aware and to defend the value aspects of personal and social life [Safa & Maple, 2016].

A number of researchers have stated in their publications that information security is still a complex issue for private users and organizations due to its multifaceted nature. Thus, N. Safa, R. Solms, St. Furnell rightly state that web technologies have brought many benefits to organizations and their clients, but the problem of information security violations still remains relevant. Antiviruses, antispam, antifishing, antispyware, brandmyers firewalls, authentication and intrusion detection systems are all technological aspects that are designed to protect information but they cannot guarantee a secure environment for the information [Safa, Solms & Furnell, 2016].

In turn, F.Belanger, St.Collignon, K.Enget, E. Negangard conclude that as currently the information is one of the most valuable asset of an organization, then attention to maintaining its security and improving the information systems is paramount; security threats related to cyber-infection are intensified both quantitatively and qualitatively [Belanger, Collignonb, Enget & Negangard, 2017].

The analysis of the considered positions shows the lack of a unified approach to understanding the essence and, most importantly, the directions of ensuring information security in conditions of total informatization and networkization of the modern society. This allowed the authors of this article to formulate the purpose of the study which is to explore the basic conceptual socio-cultural features of the essence and ensuring the information security in the information society.

Presenting main material

Thus, as noted, at the present stage of the information society development, the problem of protecting the consumer subject of information from harmful information influence is of particular importance.

One of the most prominent information society theorists, Alvin Toffler, first described the negative effects of informatization and the symptoms of information stress [Toffler, 1997]. The characteristic of the information age, according to A. Toffler, is an increase in the rate of production and dissemination of information. The high rate of informatization (or, in A. Toffler's terminology, *excessive stimulation*) requires from the subject a new level of adaptability that is not yet available to him. The subject (a person, a society), lacking the necessary strategies to overcome this information crisis, is prone to the illness that A. Toffler calls "future shock", and which we call information stress. This illness is "a human response to excessive stimulation" [Toffler, 1981]. He describes three levels of overstimulation that affect a subject's behavior:

- Cognitive level (at this level of consideration there is an overstimulation of the mental activity of the subject, which diminishes his/her ability to select, evaluate the information, resulting in information stress);
- The level of decision making (excessive flows of information cause stress to the subject, which prevents him from making any decisions when it is necessary);
- Sensory level (at this level the subject's emotions are stimulated excessively when the latter receives a great deal of new information, thus, the accuracy of the image transmission is reduced, and, as a result, the barrier between real and virtual worlds vanishes).

A. Toffler also describes four strategies for the behavior of a subject prone to the information stress. They have a negative connotation because they are the result of poor adaptation of the subject to stress [Toffler, 1981]:

- Super-facilitator strategy (the subject tries to find one common solution to all

problems, which also does not lead to the desired result);

- Revisionist strategy (a constant return to the strategies that may have helped the subject in the past but are not appropriate in the present situation);
- Specialist strategy (it is to ignore by the subject of all unnecessary information, except for the direction examined, but such specialization may be outdated under the influence of unknown external and internal factors);
- A barrier strategy (a person tries to exclude unwanted reality, remove the entire flow of new information; the subject who uses this strategy tries to adapt to the changes, but still will experience symptoms of stress).

A. Toffler points out that in this situation it is necessary to develop new acceptable strategies for the future survival of the subject (a person, a society), one of which should be the development of information literacy.

The issues of information literacy of the subject in foreign literature have often been discussed in conjunction with deep, thoughtful reading. These questions are most fully elaborated in S. Birkerts' monograph "Guttenberg's Elegies: The Fate of Reading in an Electronic Age" [Birkerts, 2017]. S.Birkerts expresses the idea that the search for truth (true) that the subject (a person, a society) is trying to find requires deep reading and deep, that is, critical, comprehension. S.Birkerts contrasts printed and electronic texts, noting that only the former is strictly linear, hierarchical, and controlled, and in the latter: "The main movement is horizontally associative, not vertically cumulative, as in printed texts" [Birkerts, 2017]. He calls the current state of total dominance of electronic texts a cognitive collage that "affects attention, the ability to read into the text, the ability to think over its complexities, the ability to extract meaning from the original rhythm and syntax" [Birkerts, 2017].

One of the central and frequently discussed issues of the information security is the quantitative and qualitative approach to information overload. A great number of foreign researchers at the end of the twentieth century took the side of a quantitative approach (linking information overload to the incredibly large amount of information at the epicenter of which there was the research subject). A. Toffler also held this position, believing that the ever-increasing volumes of new information provoke future shock [Toffler, 1997]. However, he also wrote that, by extracting and structuring information, it is possible to extend its rigid boundaries, and after that the subject is able to critically comprehend it (he wanted to say that, by improving the quality of information, it is possible to remove quantitative restrictions to some extent) [Toffler, 1981].

Among foreign researchers of information overload, there were also supporters of a qualitative approach. Among them were B. Milton [Milton, 1989], R. Owen [Owen, 2017], M. Hill [Hill, 1999] and others. They stated that the cause of information stress was not the excess of information, but rather the appearance of large amounts of low-quality information, which make it impossible for the subject to think critically, i.e. to transform it into knowledge. In particular, in the context of threats to the secure development of the information society, B. Milton argued that "one of the ironies of the new information age is that the first thing to always start talking about information is that we have too much of it ..." [Milton, 1989].

However, B. Milton states that there cannot be too much information, there is simply a huge amount of unnecessary information that forces the subject to know less than he knew before receiving it. Information is only a raw material, and decisions are made on the basis of knowledge, wisdom, intuition and understanding, that is, the products of its processing [Milton, 1989].

R. Owen also opposes the quantitative approach. In his view, it is impossible to draw a clear line of the information perception, since the subject has many resources to process it, each with its own limitations. He realizes that this limit, that is, the boundary amount of information that the subject can critically comprehend, depends not on its quantity but on the skill of processing it. [Milton, 1989].

Today, it becomes clear to most foreign researchers that the cause of information stress is not due to the amount of information as a resource, but due to the poor quality of its processing. The essence of the problems associated with ensuring information security of the man and society is that the information sphere is expanding more and more every day, both in volume and in modern means of information processing. Thus, a person loses the ability to control what is happening, and that leads to an increase in his internal tension and the emergence of stressful situations.

Current trends in the information sphere can cause different personal and social anomalies, which will inevitably threaten both personal and public security.

As the information sphere is mastered, a person on his/her way encounters certain difficulties, some of which he or she has to solve independently. This leads to the problem of formation of information culture in the subject, on the level of which depends the ability of a person to adequately respond to changes that occur around him/her. The current pace of information technology development has exceeded all expectations and refuted even the most daring forecasts [Baranov, Mamychev, Mordovtsev, Danilyan & Dzeban, 2019]. The capabilities of the equipment are now growing much faster than expected in numerous predictions of ten years ago. As a result, the relevant infrastructure, which was built on the basis of yesterday's forecasts, today is proving to be incapable of facing an information explosion. An essential feature of ensuring the information security in today's context is networking practices that are defined by functional value, but not the place where the subjects are. Places (territories) are now defined as derivatives of the functional nodes of the information network. In other words, decisions are made online, but implemented locally and territorially. An 'on-site' event becomes derived from an event in a network node. This feature is in the basis of practices of both the ensuring information security and making an aggression, such as hybrid wars. For example, today an aggressor can wage information wars in any territory, being in a convenient place for him and at any time, being anonymous.

Many modern domestic researchers [Ishchuk, 2012; Pyvovarska, 2015 & Prudnykova, 2015] believe that the Internet has actually the status of a full-fledged subculture, because it has the necessary characteristics that allow to note the formation of a full-fledged Internet culture: own slang, internal hierarchy, a set of established ideas, which in the total form the outlook of members of the subculture, certain ethical standards, a sufficient number of formal and informal leaders, who create stable communities of users around them, etc.

Indeed, if we talk about the livelihoods of local, personal networks of a social nature or micro-networks, then the claim about cyberspace as a formed subculture has its foundation. It can be claimed that the formation of personal micro-networks is a common feature of networking

practices for the information security, as well as a universal way of influencing functional macro-networks.

Freedom is a significant part of the security issues in today's information society. The information society predetermines and produces a more complex, reflective comprehension of freedom - "paradoxical freedom". Its essential characteristics are the inevitable imposition and assumption of responsibility for the obvious and latent consequences of the risks: the social subject is put in such conditions of life, when it is necessary to choose constantly, one simply cannot not choose something or someone taking into account the factor of immediate or delayed, explicit or latent risks. The assessments of the choices made vary widely across socio-cultural space and change over time. The choice that is functional, effective for one cultural space is not universal for other cultures. Deviation in one value-regulatory space becomes an innovation in another. The "freedom of risk" becomes the norm of ensuring security practices.

As L. Swedsen points out, that the circumstances of personal freedom have undergone tremendous changes. Standards of life, excess of time and material resources in modern times have become accessible not only to a small minority, and this transforms freedom of choice into one of the central concepts of human existence [Svendsen, 2016].

It is possible to agree with the thesis that the problem of innovative risks lies in the systematic insecurity of the person against the threats caused by modernization, and they are the consequences of the irrational use of the achievement of scientific and technological progress [Chuprov, Zubok & Uilyams, 2001]. On the other hand, human insecurity is caused by the paradoxical nature of individualization in a society the roots of which lie in the nature of life in the context of a "fluid present". Today, the growth of individual's isolation, individualization, deepens the imbalance between individual freedom and security.

In our view, this is due to some shift in the focus of society from norm to value. In today's cyberspace, a value orientation rather than a norm orientation is being more developed. On the other hand, the lack of a unified value system is another feature of the network "social order" that generates diversity and the development of tolerance. Present day is characterized by a focus on new selection methods that imply stability and security in the future.

The Internet is the space of highest density and intensity of communication. Different types of social structures, formed by the orientation, density and intensity of information flows condition different forms of coordination in society. It is in the social space of the network where the pressure from deviance increases and transforms faster. Therefore, we believe that cyberspace is the epicenter of the growth of various information threats to meet personal and societal needs.

Cyberspace can be seen as a space of "comfortable anomie" where comfort is determined by the peace, security and anonymity of the subject. N.Chebotariova lists a number of features of the Internet as a communication medium [Chebotareva, 2016], which, in our opinion, directly affect the security status of the subject in the information environment of modern society:

- Anonymity encourages a play with personal self-presentation and provides the opportunity to manage the impression of oneself, "escape from one's own body", promotes psychological relaxation, non-normativity in manifestations of greater freedom of expression and actions, in the reproduction of unenacted off the network activities, roles and scenarios;
- Originality of the processes of interpersonal perception: territorial accessibility and physical attractiveness lose their regulatory importance and communication is built on the similarity of attitudes, beliefs and values;
- Voluntariness and desirability of contacts, possibility of their interruption at any moment;
- Complexity of the emotional component of communication and, at the same time, the persistent desire for emotional filling of the text.

The feature of anonymity of the Internet communications has several facets: due to the physical absence of participants in the act of communication, one can express feelings, hide them, as well as express feelings that a person does not currently feel; a number of barriers to communication loses the value conditioned by gender, age, social status, external attractiveness or unattractiveness, as well as the non-verbal component of partners' communicative competence; there is an opportunity to create for themselves any impression according to their choice, while the opportunities for not only self-expression, but also for the designing of their image of their choice enrich.

Anonymity and protection from the evaluations by social network users leads to the development of abnormality and potentially causes a special state of anomie. Even if a person knows that he or she is being watched, the virtual world seems anonymous to him/her because these observations are visual. The ability to speak on behalf of another person leads to the sense of anonymity, the sense of loneliness in the crowd. In addition, anonymity provokes special emotional coloration of behavior in the Internet. Information behavior of a social subject in the modern world can be active and passive, which is determined by the level of his or her information culture. Ensuring the information security of the subject is related to the level of his or her information culture, and the higher this level, the less troubles a person has with the information and information technologies that affect him or her. On this basis, it can be argued that the level of information culture of the subject is directly proportional to the level of information security and, the higher the level of information culture, the less threats to the latter.

Conclusions

Thus, the information security is one of the acute socio-cultural problems of modern society, which is systemic in nature and concerns the activities of major institutions and subsystems; the key socio-cultural processes that take place in the society are in the context of its influence. Major risk factors for the information subsystem of society are large-scale socio-communicative and socio-cultural transformations, which have a number of negative social consequences. In recent years, there has been a clear record of disorganization-dysfunction trends that are directly related to high rates of change in the information.

Traditional practices of the information security and the security against the information are complicated due to the development of cyberspace virtual social reality. Modern communication processes lead to the information redundancy and a widening of the "fissure" between the virtual and real worlds, which is reflected in the growing convention of network practices of the information security.

The excess of low-quality information that is observed at this stage of the information society development is not the only problem of ensuring the information security. This problem also

includes the problem of the formation of an appropriate level of information culture in a person, which would prevent the emergence of stressful situations when working with the information and information technologies.

Developing in the subject the appropriate skills to work in the information field is a task of not only of the education system, the problem, which is widely spoken today, but also of each individual. Therefore, ensuring the information security in a modern society depends on many factors, including how a person will behave in a particular stressful situation.

Information security in conditions of the information society is both the protection of information and protection against information. Ensuring the information security is a necessity that becomes an attribute of the modern life of any social subject and requires continuous work with the information, which includes interaction with different expert systems, delocalization of actions, ensuring freedom and minimizing risks. The preservation of information sovereignty, the formation of an effective security system in the information field is also a pressing issue for Ukraine, which is often the subject of external information expansion, manipulative propaganda technologies and destructive information invasion. Protecting the national information space from negative information and psychological influences, guaranteeing information security and information sovereignty are of particular importance and become the factors for preserving Ukraine's national identity and functioning as a sovereign and independent state.

References

Baranov, P. P., Mamychev, A. Yu., Mordovtsev, A. Yu, Danilyan, O. G., Dzeban, A. P. (2019). Doctrinal-Legal and Ethical Problems of Developing and Applying Robotic Technologies and Artificial Intelligence Systems (Using Autonomous Unmanned Underwater Vehicles). *RELIGACIÓN. Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina*, *Vol. 4, Issue 19, 1105-1113* [In England].

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

Birkerts, S. (2017). The Gutenberg Elegies: The Fate of Reading in an Electronic Age. URL: http://archives.obs.com/obc/english/books/nn bdbirk.html [In England].

Chebotareva, N. D. (2016). Internet-forum kak virtualnyj analog psihodinamicheskoj gruppy. URL: http://ezotera.ariom.ru/2006/05/24/chebotariova. html [In Russia].

Chuprov, V. I., Zubok, Yu. A., Uilyams, K. (2001). Molodezh v obshestve riska. Moskva: Nauka [In Russia].

Crabtree, C., Nelson, M.J. (2017). New Evidence for a Positive Relationship between De Facto Judicial Independence and State Respect for Empowerment Rights, *International studies quarterly. Vol. 61, Issue 1, 210-224* [In England].

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

Hill, M. W. (1999). The Impact of Information on Society: An Examination of it's Nature Value and Usage. London: Bawker [In England].

Ishchuk, S. M. (2012). Internet-komunikatsii v konteksti kultury informatsiinoho suspilstva: *Extended abstract of candidate's thesis*. Kyiv [In Ukrainian].

Islama, M., Watson, 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* [In England].

Khyzhniak, L. M. (2017). Mify pro sotsialnu statystyku, profesiina pidhotovka sotsiolohiv ta informatsiina bezpeka derzhavy. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia: Sotsiolohichni doslidzhennia suchasnoho suspilstva: metodolohiia, teoriia, metody – Bulletin of the V.N. Karazin Kharkiv National University. Series: Sociological studies of modern society: methodology, theory, methods*, Issue. 38, 92-95 [In Ukrainian].

Markozova, O. O. (2016). Dosiahnennia zhyttievoho uspikhu liudyny v umovakh informatsiinoho perevantazhennia. *Visnyk Natsionalnoho universytetu «Iurydychna akademiia Ukrainy imeni Yaroslava Mudroho». Seriia: Filosofiia – Bulletin of the National University "Yaroslav the Wise Law Academy of Ukraine". Series: Philosophy. 4 (31), 175-182* [In Ukrainian].

Milton, B. G. (1989). Making Sense or Nonsense: Key Issues in the Information Age. *Canadian Vocational Journal*, Vol. 24, 3, 5-9 [In England].

Owen, R. S. (2017). Clarifying the Simple Assumption of the Information Load Paradigm. URL: http://www.acrwebsite.org/search/view-

conference-proceedings.aspx?Id=7387/ [In England].

Prudnykova, O. V. (2015). Informatsiina kultura: kontseptualni zasady ta svitohliadnyi sens: monohrafiia. Kharkiv: Pravo [In Ukrainian].

Pyvovarska, K. S. (2015). Virtualni sotsialni merezhi v kontynuumi Internetu: sotsialno-filosofskyi analiz: *Extended abstract of candidate's thesis*. Київ [In Ukrainian].

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

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

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

Svendsen, L. Fr. H. (2016). Filosofiia svobody. Lviv: Vydavnytstvo Anetty Antonenko; Kyiv: Nika-Tsentr [In Ukrainian].

Toffler, A. (1981). The Third Wave. Toronto (etc.): Bantam Books [In England].

Toffler, A. (1997). Futuroshok. Sankt-Peterburg: Lan [In Russia].

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