Rasim M. Alguliyev[1], Yadigar N. İmamverdiyev[2], Rasim Sh. Mahmudov[3]
[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]secretary@iit.ab.az, [2]yadigar@lan.ab.az, [3]rasimmahmudov@gmail.com

DOI: 10.25045/jpis.v08.i2.04

MULTIDISCIPLINARY SCIENTIFIC AND THEORETICAL PROBLEMS OF INFORMATION SECURITY

The article investigates the multidisciplinary scientific and theoretical problems of information security. It particularly analyzes the international, political, psychological, legal, economic, cultural and ethical aspects and issues related to training and child protection. Current research directions in these areas are determined.

Keywords: *information society, information security, information and psychological security, information war, information security culture, information security of children.*

Introduction

Nowadays, the process of formation and development of global digital environment and virtual relationships is underway influenced by the information and communication technologies (ICT), especially the Internet. The relationships between the public administration, economic activity spheres, science and education system, information and communication environment, and all areas of private life and business are transformed from the traditional environment into the virtual one. Humanity faces a new situation, i.e. a system of relationships that has no analogues. Transition into the virtual relationships poses a number of problems, along with the benefits that it brings to humanity. In this situation, there is a great need for new security techniques and tools.

At the beginning of the third millennium, information security becomes crucial in the national security system for its significance. Thus, information has become the most valuable resource of humanity, and all progressive innovations in science, education, governance, economy, business, society, and important events are related to information and knowledge production. In the information society, all spheres of human activity are transferred into the information space, and the information processes cover social, political, legal, economic, psychological and cultural relations. In addition, the negative effects of information flows become more prominent, with cybercrime, cyber-terrorism, and information war threats [1].

It should be noted that information security has always existed since the creation of mankind. As the civilization develops and the information revolutions follow one another, the information carriers and their capabilities have begun to increase. The information on paper was controlled by humans, and therefore was dependent on their will. Even if the information was out of control of a human, its multiplication, spreading speed, and the scope of impact were often limited compared to current possibilities. In the modern era, the diversity of information carriers and sources, along with all the positive sides, poses serious threats to information security.

According to unanimous conclusions of the scientists and experts working in the relevant field, not only the complex technical components of the information security system, but the human factor must be taken into account [1]. Information security issues are not limited to the provision of the availability, integrity and confidentiality of the processed information. The impact of information on human beings and the decision-making (humanitarian) issues should also be taken into consideration.

Thus, humanitarian problems, which are often presented as the technological challenges, often require a range of information security solutions. However, existing research and practices focus on the technical and technological aspects of information security rather than the humanitarian aspects of the problem. In this regard, there is a great need for a multidisciplinary research in the field of humanitarian problems of information security.

The presented study identifies the multidisciplinary scientific-theoretical problems and key research areas of information security, and proposes multidisciplinary recommendations on the formation of the information security system.

Political aspects of information security

The political problems of information security cover the spread of information warfare, the dissemination of electronic intelligence and state secrets, dissemination of incorrect information and disinformation about important events and processes realized in the interests of the domestic and foreign political forces.

Different public-political communities aimed at changing the constitutional order and integrity of the country by force, the activities aimed at encouraging the social, ethnic, regional and religious aggression are regarded as more aggressive threats to the domestic politics [2].

To ensure information security in the domestic policy, the mechanisms to prevent the disinformation about the state policies, authorities, and officials should be developed and implemented.

The important targets of the information security in the field of foreign policy are the information resources of the state authorities, diplomatic representatives in foreign countries and international organizations.

It must be noted that, virtual space traditionally opens up opportunities for the contradictions between the peoples, countries, and religions. The virtual space has no certain borders. All states are equally close to each other here. Therefore, an information war and attacks are possible in the virtual environment anytime and anywhere.

Today, the special laboratories of power centers with global political allegations synthesize ethno, national and religious threats and conflicts for different regions and countries based on the multidisciplinary scientific approach. The synthesis process of these hazards involves historians, sociologists, conflictologists and other experts. Certain laboratories detect the damaging effects as *domino, butterfly,* and *snowball* by analyzing the contradictions in targeted regions and countries and synthesize the strongest information weapons [1].

In general, the scientific aspects of information security in the following areas are of great importance:

- scientific-theoretical problems of the formation and development of the information society;
- global information space, information imperialism and sovereignty of the national states (information);
- national interests of the states and information confrontations in the modern world;
- concepts and technologies of information warfare, problems of formation of information troops;
- values of society and modern information threats targeted at them;
- information security policy, priorities and strategy of the state;
- information security in the context of state bodies, political authority, society and identity;
- information security of political communications and political ethics;
- public control over information and information security, and civil society mechanisms.

Features of information and psychological safety

Information and psychological security is understood as the protection against the influences of the harmful information that can change the mental state, psychological characteristics and behaviors of the individuals, social groups and human communities against their wills and desires.

These threats are targeted at the mentality and national-moral values of a whole nation and people. Given the fact that these values are of the key factors that form and strengthen a state, the level and scale of these hazards can be deeper understood. Specifically, the degradation of the mentioned values of the Azerbaijani society destroys the fundamentals of the family institution. The family institution acts as the main support and regulatory mechanism of the society. These values are affected (corroded) by these information and psychological impacts. Instead, the axiological values of people - national and moral values are spoiled, historical and modern influential people are discredited, the institution of the family are destructed, the cosmopolitan feelings and the sense of humiliation for the past are instilled.

Compared to other types of impact, the information and psychological impact has some distinctive features as follows:

- having a broader impact on the country (reducing the development pace, creating large-scale conflicts between the countries, ethnicities and other human communities, forming a dictated lifestyle in a large region, directing the management to desirable figures);
- capable to prepare long-term, multidisciplinary, complex and staged programs of information and psychological impact, which generate large dividends with small financial costs;
- having high privacy;
- lack of effective international and national remedies to protect these effects.

The abovementioned features of the information and psychological impact confirm that the most dangerous weapon of the 21st century is the weapon of information.

Experts distinguish the main three groups of reasons for the exposure of the citizens, social and the general population to information-psychological impacts:

1. Political factors (change of the geopolitical situation after radical changes in different parts of the world, and the emergence of new national interests; emergence of new statehood in the terms of democracy, legality and information openness; collapse of existing team-administrative and political-administrative systems; information expansions of developed countries for the dissemination of the Western outlook, political and moral values; strengthening the international cooperation; low level of political, legal and information culture in the society).
2. Socio-economic factors (difficulties in transition to market economy; sustained inflation and decline in living standards; increase in unemployment; breakdown of the previous social structure; deepening of the differentiation in the society; increasing tension in ethnic relations in the society, the criminalization of crime, drug addiction, alcoholism, immorality, and social relations; deterioration of the health status of the population).
3. Moral factors (crisis of the state ideology; deformation of the public norms and values system; emergence of new forms of influence on individual, group and mass consciousness (including media and Internet technologies); poor assessment of the national and cultural-historical traditions and the effects of Western cultural templates on the public consciousness; destructive effects of non-traditional religious confessions, weakening of important social and cultural institutions (science, education, culture) of the state.

The solution of information-psychological security problems necessitates the researches in the following areas:

- development of the initial typology of threatening information effects; systematization of the diagnosis of such effects based on accepted and applied criteria; classification of the methods of the psychological protection of identity, community and state information threats;
- analysis and development of proposals for correcting appropriate methods and practices for enlightening and educating the children and adults; development of personal and group protective tools from manipulative and esoteric psychopathic and psychotechnical methods applied in electronic media and the Internet;
- organization and implementation of the psychological examination of information products;
- establishment of a psychological consulting system for the developers and users of the information products.

In recent years, the role of public opinion has greatly increased in the socio-political processes and the psychological state of the population related to the development of electronic media. Therefore, the public opinion formation system should become one of the main objects of the provision of information-psychological security. From this point of view, it is necessary to study the characteristics of the formation and deterioration of the public consciousness. Furthermore, the psychological models of the system of the information-psychological impact, and the diagnostic tools of the prevention monitoring and methods of the appropriate effects should be developed.

Information security and globalization

Before the Internet, the socialization took place very long. Therefore, the development rate of the civilization was low. Now, many opportunities have been created for the development of civilization and the emergence of flexible socialization. These processes are rapidly developing, consequently, science, education, technology, culture, economy, and law system are generalized and globalized.

The globalization process accelerates the transition from the national statehood to the global society. The globalization mainly focuses not only on the states and transnational companies, but also the ordinary people.

The globalization of technosphere leads to the formation of a single international technological and information medium. The social and cultural globalization, which takes place in the fields of science, culture, education, ethics and ideology, brings a new wave of unification and standardization to the spiritual sphere.

The globalization processes open up new perspectives in all areas of human activity and at the same time creates favorable conditions for serious threats. New threats to the globalization in the field of information security can be summarized as follows [5, 6]:

- interstate contradictions and conflicts are transferred to the information space; information contradictions are strengthened; information weapons are used; information wars are aggravated;
- infogen disasters occur as a result of accidents and misfortunes in global information and communication networks;
- global information infrastructure emerges, where it is difficult to controlled the criminal organizations and networks;
- new types of crime inherent in the global virtual environment emerge;
- large amounts of personal data are illegally collected for criminal purposes;
- total manipulation of public consciousness is possible.

The problem of ensuring information security in the context of globalization is of international, complex and multidisciplinary character. The solution of this problem directly depends on the quality of relevant scientific and methodological foundations and the level of international cooperation between the countries.

International co-operation may cover legislation, struggle with cybercrime, respond to incidents, scientific research, and hardware and software certification. However, in this strategic area, risks of economic, political and national security are also possible in the cooperation with foreign countries.

The problem of global information security was first mentioned in the Okinawa Charter on Global Information Society, adopted by the G8 leaders in 2002. At the next stage, the final documents of the World Summit on Information Society highlighted the need for real measures to ensure the safe use of ICT at the global, regional and national levels.

The UN plays a particular role in ensuring information security at the international level. The UN General Assembly has adopted five different resolutions on information security since 2000. Moreover, Organization for Economic Cooperation and Development, the World Telecommunication Union, and European Union Agency for Network and Information Security also develop regulatory and methodological documents and recommendations on information security [7].

Relevant legal basis should be established to ensure information security at the international level since the effective cooperation among countries is essential.

Legal problems of information security

In the information society, people are citizens of their countries, bear responsibility for the laws of the state they belong to and realize their rights and obligations. They also become a virtual citizen of a new world, i.e. the virtual world. In this new world, a generally accepted system of law has not been formed yet. In addition, there are a number of problems related to the legal regulation of information security in the virtual environment.

The main objective of the legal regulation of information security is to eliminate the threats to the national interests in the information sphere and to minimize the losses from these threats. One of the important areas of legal security of information security is conducting relevant research. These researches should cover the study of the following areas: the legal aspects of national interest in the information field, the legal tools and mechanisms that provide effective countermeasures against these threats, the cooperation opportunities in various fields of law to deal with the relevant subject area, the relations between the international and national legislation related to the relevant regulation.

Obviously, the legislation on information sphere does not have analogues in the history. Therefore, along with the lawyers, IT professionals, psychologists, sociologists, and educators should attend the development of relevant legislation.

The development of the regulatory framework in the field of information security is a very difficult and complicated process. This is due to the fact that the relevant regulatory framework is created to control social relations, which is still being formed, accompanied by contradictions. In fact, new giant media volumes are now beyond legal regulation. There is a need for a comprehensive study of the problems in this area and for the development and implementation of the real targeted strategies.

The formation of a legal framework in the field of international information security is a rather slow and complicated process. As with other issues, the international community is facing a typical problem, i.e. the interests of the countries do not coincide.

The international law also has some problems with information security issues. First of all, it should be noted that, international law has enough gaps in the sphere of information related to the universal recognition of the essence of international security. At present, the negotiations between the countries do not resolve this problem. For example, there is no general view of the assessment of an "aggression act" implemented by any country against another one by using ICT or media as a weapon. According to this aggression act, the visions of the jurisdiction of any state to be applied for self-defense are also controversial [7].

One of the major problems in the field of legal security of information security is related to the formation of a standard terminology. The international law does not have sufficient terms that can define the processes occurring in the field of information security. Moreover, the number of issues in the information sphere that can pose a threat to international security is substantially increased. However, not all of them can be explained with the existing legal terms.

The most difficult issue is the impossibility of information security in the framework of the jurisdiction of any country.

Factually, the use of ICT for criminal purposes is subject to the characteristic of the international law specified by the Charter of the United Nations. Thus, "threats of force", "use of force", "territorial integrity", and "state sovereignty" are envisaged in this UN document. Nevertheless, the international law does not refer to ICT as "tools" or "means" of "enforcement threats" or "use of force".

The use of media for criminal purposes, such as influencing the domestic policy of the state, changing its territorial integrity, or violating the state sovereignty, is not a subject of the international law.

Economic problems of information security

However, information security is perceived as a technological field of activity, some problems in this area are associated with more economic factors. As in any area, the economy of information security also has its own peculiarities. The economy of information security economy is an independent area of economy, although it is linked to a number of common economic laws and methods.

The increasing role of information in the society, including the economy, intensifies the interest in information security in economic sciences. In economic sciences, information security is referred primarily in terms of economic interests of the enterprise and the state.

One of the most important aspects is that the assessment of the economic value of the application of information security tools. Here, an analysis of the economic effectiveness of the costs involved in the provision of information security of the enterprise is the main research object [8].

The assessment of information security risks and threats is another trend. This trend incorporates the classification of information security threats and the systematization of information risks. In addition, the development of the methodologies for information risk assessment and analysis can also be referred to this trend.

Perspective aspects of the economy of information security include the creation of a system of information security risks insurance for individuals and legal entities and the development of economic methods of struggling with information security threats.

In general, scientific research in the field of economic information security should be conducted in the following trends [1, 9]:

- information security of modern social and economic systems;
- assessment of information security risks (including the value of information and information resources and the damages);
- models of information security risk insurance;
- modeling of investments in information security;
- evaluation of the vulnerability of certain sectors of the economy to cyber-attacks;
- information security of e-services, including e-commerce;
- resource allocation models for information security;
- economic regulation of property relations with information resources.

Human resource training in information security

Statistical data of the recent years show that most of information security violations occur due to the human factor, i.e., failure to follow safety procedures, human error, inadequate training, and lack of knowledge in information security.

It should be noted that the human factor depends not only on the professional competence, but also on the personal qualities. The personal qualities may include the ability to follow the ethical norms while performing professional duties, being disciplined, honesty, adherence to principles, responsibility, and emotional stability, self-control, keeping secrets, avoiding harmful habits, attentiveness, and sociability [1].

Currently, information security education focuses on training and retraining of human resources on technical aspects of information security. At the same time, there is considerable retardation in the field of training the specialists on information law, methodology and organization of computer crime investigation. To successfully fight the cybercrime, it is necessary to adopt the curriculum on the training of the professionals both in computer crime investigation and information security [10].

The demand for highly qualified specialists in the field of information security can only be met through the comprehensive use of the opportunities of secondary, higher and additional vocational education. The corresponding demand can also be provided by ensuring the permanent educational process.

One of the important issues in the relevant personnel training process is the establishment of close relationships between the teaching process and the information security research. Obviously, the quality of teaching depends on the depth of the relevant scientific research. Excessively scientific IT technology requires the highest level of the specialists in this area.

Another important issue is the content of the curriculum. The content of relevant curricula should be updated once a year (at the start of each academic year) to ensure the latest achievements in the field of information security.

One of the problems arising in the training of information security workforce is the logistical support of the teaching process. Practical and laboratory workshops should be conducted in the places specially equipped with the introduction of modern technologies.

Training in the field of information security should be carried out not only in the technological field, but also on different aspects of information security, i.e., highly qualified lawyers, doctors, psychologists, journalists, sociologists, technologists and political scientists in the field of information security should be prepared.

Information security culture

In the information society, the importance of information culture in the context of common cultural norms is increasing. Information culture is the ability to use modern ICT to search, receive, store, process, analyze and provide the needed information and ensure its completeness, objectivity, confidentiality, legal and ethical compliance [11].

One of the components of information culture is the information security culture. In this regard, the most effective anti-threat strategies is to form a culture of information security of the citizens.

Information security culture is the ability to protect personality from harmful information and psychological impacts and to ensure the security of its information. In addition, the culture of information security is the process of continuously improving the personality and its information by creating and maintaining the level of protection against harmful effects through existing knowledge, attitudes and skills. It is also the process of a complete improvement resulted in the provision of information needs [12].

Technical knowledge and skills on information security, information effects harmful for moral and psychological health of a human and the knowledge and skills on the methods of protection against them, and following the legal and ethical norms when using information resources are the core of the information security culture of the human.

One of the most important mechanisms for the formation of the culture of information security is to educate the civil servants about the proper assessment of safety, the use of information technologies responsibly, and the adequate response to the incidents related to the information security breaches. Unlike non-governmental organizations, the civil servants need to be more tolerant to the harmful information and psychological effects.

The process of forming the culture of information security in the state bodies should be of comprehensive character and include the process of creating a corporate and information culture. The following measures should be taken to establish and improve the culture of information security in state bodies [12]:

- strengthening the relevant legislative framework;
- developing and proper implementation of the guidelines for formation and use of national information resources;
- establishing the organizational, personnel and resource bases for the monitoring system of the information security threats in the state bodies, and using their capabilities in the

assessment of the information security of the state structures;
- improving the system of control over the civil servants' performance related to information;
- increasing the rate and organization of civil servants' training, and developing the special training programs on information security.

Forming of information security culture in non-governmental organizations is also crucial. The information security culture of an organization implies the respect for the common interests of all employees in the organization concerning the information. This is the common interests of the business owners, founders, customers, partners, managers and employees. The relevant behavior is one of the key conditions to support the mutual trust-based relationships of the parties with common interest in the strategic perspective.

In general, scientific research in the following areas is urgent within the context of the formation and development of information security culture [10]:

- main aspects of the state policy in the field of information security culture;
- awareness of the population about information security issues;
- content and structural components of information security culture;
- mechanisms for the formation of information security culture;
- formation of information security culture in organizations;
- measurement (identification of indicators) of information security culture.

Information security ethics

Ethical norms play an important role in ensuring information security. Self-regulation based on the moral and ethical standards is one of the most effective ways to protect participants from antisocial behavior. Moral and ethical norms of the society can play a key role in creating new legal regulations and improving existing ones in the future. Thus, the ethical norms that correspond to the reality posed by the information society can act as the guarantor of the information security of the identity, society and state.

The importance of this new information security institute has led to the emergence and significance of a new field of research, i.e., information ethics. Information Ethics studies the peculiarities of the social impact of the computer technology on the society and the moral norms formed based on these technologies and the consciousness of their developers and users. Information Ethics is a field of science and knowledge that combines professional ethics, consumer ethics, and some issues of the state policy [13].

At present, most technologies affecting the professional ethics of any field of knowledge are related to information. This circumstances cause high demands for professionals - programmers, system administrators, and information security analysts.

The International Federation of Information Technology has recommended the adoption of a code of computer ethics based on the ethical standards specified in the codes of the relevant organizations of other countries. These standards are based on 10 basic principles, taking into account the local cultural and ethical traditions [14].

All relevant codes urge to honestly fulfill the duties based on the fulfilment of four basic moral and ethical principles (privacy, integrity, private ownership and availability); professional and social responsibility; increasing the qualification; ethic norms such as race, religion and ethnicity.

The 36th UNESCO General Conference in 2011 adopted the Code of Ethics in the Information Society. This document proves that, as in real life, the rights and freedoms of people should remain unchanged in the information space [15].

The education system has important tasks in the formation of the information security ethics among the participants of the information relationship. Students should be aware of the legal, social, and ethical aspects of information security.

Information security of children

Information streams strongly influence the children in the information society. Children acquire the filtered information from the surrounding environment: from the Internet, media, various communication tools and communicating people. Studies on the information security of children show that there are still some unresolved problems in this area. The solution of these problems, first of all, requires multi-aspect and multidisciplinary approach to the issue. Experts believe that the information security of children has groups of threats related to the physical health (criminalization of information space, failure to follow computer rules and regulations), psychological situation (manipulation of consciousness, dependence on computer and network games, cyberbullying, trolling, threatening, humiliation), spiritual development (impact of prohibited information for children, the main threats related to trafficking in human beings, the effects of violence, involving to extremism and terrorism, restriction of information rights, non-ethical behavior in social networks), and material loss (private data theft, malicious software effects, illegal purchase though the Internet, copyright infringement) [10].

It is necessary to create a safe information and educational environment to ensure the moral, physical, psychological and social health of children. The following measures must be taken in this regard:

- establishment of appropriate organizational and legal mechanisms to protect children from the spread of information damaging their health and development;
- application of systems restricting the access to information preventing children from being educated as citizens, data filtering tools and other appropriate hardware, software and technological facilities;
- prevention of Internet addiction of children, providing the knowledge and skills to children to be responsible and safely behave in virtual environment;
- enlightenment of the parents about the methods to protect information damaging the children’s health and development;
- provision of information security for all categories of listeners, and inclusion of behavioral issues into curriculum;
- psychological and pedagogical features of the informatization process of education, and the organization of special courses for pedagogics and psychologists on the prevention of negative impact of ICT on a child identity;
- development and implementation of special courses for classroom manager, kindergarten educators and social educators with families on information security issues;
- development and implementation of information courses for parents to protect their children from harmful information;
- provision of all educational institutions and electronic libraries with software products that ensure the content filtering of the Internet traffic;
- performance of the content filtering by the Internet providers in transferring the Internet traffic to the educational institutions.

It should be noted that it is impossible to provide the children's information security on the Internet without the involvement of the parents. The reality proves that many parents do not realize the existing and potential dangers for children on the Internet. Therefore, it is important to combine the efforts of parents and educational institutions to ensure the information security of the children on the Internet.

Conclusion

The study of humanitarian fields of information security shows that these areas are a new and extremely complex, multifactorial subject of multidisciplinary scientific research. All of this requires the combination of efforts by humanitarian and technical scientists and experts in the field of information security. Such cooperation can play an important role in the development of complex measures to ensure the secure information security.

Information security issues are not limited to the justification, completeness and confidentiality of the information to be processed. The political, legal, economic, psychological and staffing aspects should be taken into account. In the information society, all spheres of human activity are transferred to the information medium. Consequently, the information processes cover social, political, legal, economic, psychological and cultural relations. Moreover, the negative effects of information processes are more prominent, and the cybercrime, cyber-terrorism, and the threat of information warfare are increasing. Thus, humanitarian problems, which require a range of information security solutions, are often presented as a technological challenge. However, the current studies and practices often focus on the technical and technological aspects of information security. The humanitarian aspect of the problem is not fully highlighted. In this regard, there is a great need for multidisciplinary research in the humanitarian field of information security.

References

1. Alguliyev R.M., Imamverdiyev Y.N. Humanitarian aspects of information security / II Republican scientific-practical conference on multidisciplinary problems of information security, May 14, 2015, pp. 9-12.
2. Alguliyev R.M., Imamverdiyev Y.N., Yusifov F.F. Some conceptual views on information security of society // Problems of information society, 2011, No2(4), pp.3-9.
3. Grachev G.V. Sociology of Information-Psychological Security: the problem of formulating the definitions // NB: International relations, 2013, No 4, pp.61-85.
4. Imamverdiyev Y.N. Problems of the Provision of Information-Psychological Security / II Republican Scientific-Practical Conference on Multidisciplinary Problems of Information Security, May 14, 2015, pp.78-81.
5. Brandman E.M. Globalization and Information Security of Society // Philosophy and Society, 2008, No1, pp.31-41.
6. Malykhina G.I., Aksenov V.V. Modern Information Security and Problems of Globalization // Science and Military Security, 2008, No 2, pp.7-12.
7. Musayev V.Y., Imamverdiyev Y.N. International Challenges, Initiatives and Obligations in Information Security / II Republican Scientific and Practical Conference on Multidisciplinary Problems of Information Security, May 14, 2015, pp. 102-105.
8. Bohme R.R. (Editor) The Economics of Information Security and Privacy, Springer-Verlag Berlin Heidelberg, 2013, 327 p.
9. Alguliyev R.M., Mahmudov R.Sh. Security Issues of Information Economy // Information Society Problems, No1(7), 2013, pp. 3-13.
10. Mjolsnes S.F. A Multidisciplinary Introduction to Information Security, CRC Press, 2011, 348 p.
11. Alguliyev R.M., Mahmudova R.Sh. Information culture: essence and formation problems, 2010, No1, pp.14-22
12. Imamverdiyev Y.N. Problems of information security culture in e-government environment // Problems of information technologies, 2015, No1, pp.80-88.
13. Chusavitina G.N., Chernova E.V., Makashova V.N., Zerkina N.N., Kuznetsova I.M. Ethical issues of application of information technologies as a component of the subject preparation of university students // Fundamental research, 2015, No 10, pp.318-323.
14. Martin C.D., Holz H.J. Non-apologetic Computer Ethics Education: A Strategy for Integrating Social Impact and Ethics into the Computer Science Curriculum, http://www.southernct.edu
15. UNESCO, Code of ethics for the information society, http://www.unesdoc.unesco.org/images/0021/002126/212696e.pdf
16. Livingstone S. Children and the Internet, John Wiley & Sons, 2013, 320 p.