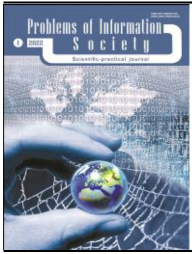

www.jpis.az

13 (1)
2022

Analysis of international experience in the formation of a culture of information security in society

Rasmiyya Sh. Mahmudova

Institute of Information Technology, Azerbaijan National Academy of Science, B. Vahabzade str., 9A, AZ1141, Baku, Azerbaijan

rasmahmudova@gmail.com

ORCID: orcid.org/0000-0002-5816-9373

ARTICLE INFO
http://doi.org/10.25045/jpis.v13.i1.10

Article history:
Received 27 July 2021
Received in revised form
30 October 2021
Accepted 10 January 2022

Keywords:
Information security culture
Culture of cybersecurity
Awareness of information security
Cyber education
Media education.
International experience

ABSTRACT

The rapid development of information and communication technologies, the increase in sources of information, the electronization of many services in all areas, the emergence of new means of communication between people, the collection of personal data in various information systems and other realities create new opportunities for development. On the other hand, the use of information to manipulate people's minds, to create chaos in society, actualizes the development of a culture of information security in society. The article analyzes the experience of developed countries in the formation of information security culture. As part of the documents, challenges and measures taken by international organizations such as the UN, the Organization for Economic Cooperation and Development, the experience of individual countries in raising the level of information security culture of professionals, citizens and various groups, as well as educators, children and youth, was studied and summarized. The study used methods of systematization, generalization, comparative analysis. The results of the study may be useful to institutions responsible for ensuring information security in society.

1. Introduction

Information has become an important and valuable component of the functioning of primary subjects of the society, i.e., individuals, economic institutions, and state. When it is impossible to prevent unauthorized access to highly important information accordingly, several problems emerge regarding the provision of the security at individual, social, and state levels. Hence, experts estimate that the formation of the culture of information security (CIS) is paramount in accordance with social realities.

Noticeably, present-day entities and organizations operate in a mutual contact in a digital environment. That creates wide opportunities for them for cooperation and information exchange. However, this mutual connection exposes them to internal and external threats at the same time. Internal threats are the most commonly encountered information security problems by enterprises [1]. Employees expose their enterprises to major threats in terms of information security deliberately, without knowing or, in most cases, due to the lack of essential knowledge.

International reports and expert opinions analysing cyberattacks estimate a human factor to be one of the key elements in the area of cybersecurity [2]. Although the management of passwords and prevention of phishing attacks are important security measures, information security culture must be at a high level in order to manage information security risks in enterprises. At present, social engineering tools are masterfully used to obtain valuable information by manipulating the minds of people [3].

Information security is a broad term and entails information-psychological security facilitating the protection of subjects from negative information influence alongside the information protection, that is, the direct provision of information security [4]. At the same time, the non-compliance with legal and ethical norms while using information resources is another information security problem.

As observed, a culture of information security is the compilation of technological culture, information-psychological culture, and legal-ethical culture in the field of information security. At present, there are fierce attempts to form global cybersecurity culture in the contemporary world. This enables claiming that the provision of information security has become one of the important global problems of our time. Leading international organizations have contributed greatly to the development of the global cybersecurity culture. The first international organization showing interest in this problem was the United Nations (UN). It is due to the prominent role of CIS in the provision of the international public security. On the other hand, the development issues of information technologies and information exchange have always been in the focus of the UN. For example, The UN General Assembly adopted the declaration "Information freedom: human rights and scientific-technical development" in 1971. The problems of CIS formation have also been in the focus of the UN that resulted in the adoption of a declaration "Creation of global cybersecurity culture" by the General Assembly on 20 December 2001 [5].

The recommendations "*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*" [6] adopted by the Organization of Economic Cooperation and Development (OECD) in 2002 has given an impetus to the formation of CIS in developed countries.

The formation of the CIS becomes a necessity in all segments of population in the environment of widespread use of the internet, high-productivity personal computers, and various mobile devices. The key principles of this culture are represented in the OECD recommendations, and those are "awareness" and "responsibility". In essence, these notions cover:

- awareness – all citizens should be aware of the need for the provision of security of information security;
- responsibility – all citizens are responsible for the security of information systems.

2. Measures to enhance the knowledge and skills of individuals and experts responsible for information security

Let's attempt to analyze the practice in skill development and assessment in the field of information security provision in economically developed countries, in particular, in the European Union (EU) and the US. The development of skills in information security bears a systematic character in the EU and is conducted systematically from the design of training programs to the development of skill assessment tools, including self-assessment.

In the EU, the European Network and Information Security Agency (ENISA, from 2019 onwards, The European Cyber-security Agency) established in 2004 is responsible for conducting various training events in the field of information security. One of the main trends of the agency's activity is the support for training and agitation activities for the secure use of information-communication technologies (ICT) in member countries and enhancement of readiness level of EU citizens.

ENISA implements various programs aiming at the enhancement of the awareness regarding information security issues. For example, the "Guidelines for new users: how to enhance the awareness on information security" prepared by the agency in 2010 is a practical guidebook for planning and conducting awareness enhancement programs in information security [7].

Regarding necessary knowledge and skills in this field, the EU recommendations prepared for citizens emphasize cybersecurity risks and related risks, i.e., misinformation, cyberbullying and radicalization. The violation of the information security in the state governance system is deemed a critical risk.

The information security assessment and training are conducted within the framework of all-European trainings (Cyber Europe). These trainings utilize technologies developed by experts specialized in cybersecurity and based on reality modelling.

The scope and systematic character of the works carried out by the EU in terms of the enhancement of digital literacy can be determined by the number of participants (18 transnational corporations, over 300 project developers and over 7 million citizens) as well as by many measures aimed at the application of the Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies (SELFIE) tool (11 types) [8].

In the United States, the responsibilities of government agencies to train all employees in the basics of information security are defined at the legislative level. The Federal Information Security Management Act (FISMA), Section III of the 2002 e-Government Law, sets out the responsibilities for raising the awareness of all employees working with information systems on information security issues. In accordance with the goals of implementation and evaluation of the information security competency development program, employees are divided into 2 groups: "information technology specialists" and "users". The verification of the effectiveness of the implementation of information security policies and procedures, as well as the verification of knowledge, are performed periodically. Requirements for improving information security and their verification methods are specified in a designated document [9].

The 2003 US document "Information Technology Security Introduction and Training Program" elaborates in detail on the basics of information security that should be communicated to all employees.

In the US, the periodic assessment of knowledge is an integral part of the enhancement of information security awareness proqram. Tests are main tools used in this case alongside sudden examinations, the use of specifically prepared notifications, and additional examination methods, such as the violation monitoring and registration of adopted information security policy.

The Cyber Security Skills Model [10] developed by the US Human Resources Administration in 2011 identifies a set of important competencies for information security professionals in various fields.

The approach proposed in this document is used to standardize the job functions performed by information security professionals in many of the US government agencies to unify the requirements for their primary specialization and to determine the need for additional education.

The document "National Initiative for Cybersecurity Education, (NICE): the structure of cybersecurity human resources" [11] dated 2017 includes a model for determining the degree required from information security specialists with various profiles who perform job tasks. The document mentions 52 functional specializations engaged in the provision of information security and provides a list of tasks for each of them, as well as shapes adequate knowledge, skills, and competences.

Currently, several international organizations are engaged in the organization and conduct of wide-scale national and transnational cyber-trainings (table 1.).

The EU occupies a special place among the aforementioned organizations; it organizes and conducts cyber-trainings based on designated documents adopted by the European Commission. These trainings are based on several documents adopted by the EU Commission.

For example, the resolution adopted by the Council of the European Union in 2009 created a legal basis for "conducting national cyber-trainings" and was a call for an active participation in international, transnational cyber-trainings. The first cyber-training by the EU was conducted in 2010 (Cyber Europe, 2010), and the joint cyber-training of the US and the EU was held in 2011.

The following include main trends of cybersecurity development set out in The European Digital Agenda on "Trust and Security" which is an integral part of the "Europe 2020" Strategy [12]:

- policy enforcement in the sphere of network and information security;
- preventing contemporary cyberattacks on critically important state and commercial information systems;
- establishing European platform for fighting cybercrimes;
- exploring the necessity for creating an European center for fighting cybercrimes;
- studying the methods of informing users in case of security system violation (loss, theft and alteration of personal data and other confidential information);
- monitoring the compliance with privacy rules on the Internet;
- supporting the mechanism of informing about illegal online content and raising awareness about safe Internet among children;
- providing a hotline for receiving information on revealing illegal contents by EU member states;
- creating national alert platforms raising awareness regarding EU-scale threats;
- etc.

Table 1. List of international organizations conducting cybertrainings

Name of organizations conducting cybertrainings	**Internet website**
Asia-Pacific Economic Cooperation (APEC)	www.apec.org
Association of SouthEast Asian Nations (ASEAN)	www.asean.org
European Union (EU)	www.europa.eu
Council of Europe	www.coe.int

Europol	www.europol.europa.eu
Forum of Incident Response and Security Teams (FIRST)	www.first.org
Group of eight (G8)	www.g8russia.ru
Institute of Electrical and Electronics Engineers (IEEE)	www.ieee.org
International Electrotechnical Commission (IEC)	www.iec.ch
International Organization for Standardization (ISO)	www.iso.org
International Telecommunication Union (ITU)	www.itu.int
Internet Corporation for Assigned Names and Numbers (ICANN)	www.icann.org
Internet Engineering Task Force (IETF)	www.ietf.org/about/mission.html
Internet Governance Forum (IGF)	www.intgovforum.org/cms

3. Raising the level of culture of information security among citizens and various population groups

As already known, one of the main problems in the development of the information society is to ensure the information security of the state, society and individuals, i.e., the members of this society. Everyone should have some essential knowledge in the field of information security to combat the growing information threats, cybercriminals, cyber fraudsters, cyber-hooligans, and etc. to be able to protect himself/herself. In this regard, users must first be aware of the dangers they may face while working on the Internet and using various electronic services.

In addition to the involvement of individuals in mass trainings and the mechanisms such as extensive advocacy work and the establishment of "hotlines" are used for the CIS formation and skill development in this sphere.

Although countries differ for the development rate of the information society, the problems of information security in almost all countries are practically the same. Approaches to solving these problems differ depending on the cultural level of the country and the national legal framework in this area.

Most countries adopt various measures, first, to raise awareness of citizens regarding threats they face in information space and protection mechanisms against these threats, and to advance the level of the CIS. These measures focus on various issues, from general information security issues to protection of personal data, electronic signature, electronic identification document, electronic health services and security risk management [13].

Awareness-raising activities cover a wide range of social groups, from ordinary citizens to professionals working in public organizations and the private sector.

In developed countries, governments organize many conferences and seminars to raise the level of CIS of civil servants, including representatives of the private sector, and sometimes citizens. One way to form an CIS is to develop and disseminate free information materials, recommendations, and guidelines. Television, social networks, and SMS notifications are often used to distribute security materials.

Countries carry out various measures to raise the citizens' awareness of information security issues (Fig. 1).

The largest project in this direction is implemented in the United States. The National Cyber Awareness System provides users with timely and useful information to support the security of their computer systems. The information system is designed for users with different levels of computer training (both professionals and ordinary users of personal computers). Moreover, the US Federal Trade Commission cooperates with several coalitions, such as Anti-Phishing Working Group, National Cyber Security Alliance, etc. for many years to better contribute to consumer education and expand the distribution of print and web publications on information security issues [14].

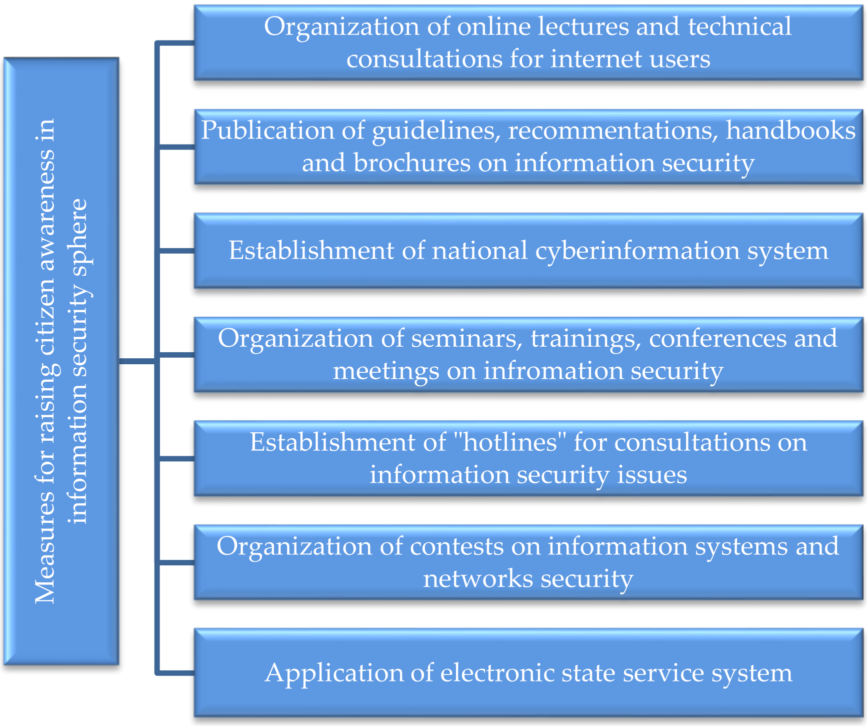
Measures for raising citizen awareness in information security sphere
Organization of online lectures and technical consultations for internet users
Publication of guidelines, recommentations, handbooks and brochures on information security
Establishment of national cyberinformation system
Organization of seminars, trainings, conferences and meetings on infromation security
Establishment of "hotlines" for consultations on information security issues
Organization of contests on information systems and networks security
Application of electronic state service system

Fig.1. Measures for raising citizen awareness

A gateway (*Consumer Information Gateway*) established in Canada provides the citizens with access to all information and services provided by both the Canadian government and non-governmental organizations. It offers a wide range of publications on cyber security, protection of financial confidentiality in cyberspace, security of electronic purchases, protection of personal data, protection against spam.

An online forum set up in Finland holds interactive discussions with citizens on information security issues. This forum offers citizens to communicate with government agencies. Members of the Government Council for Information Security Management are actively involved in the discussion of information security issues.

It should be noted that the Ministry of Transport and Communications and the Data Protection Ombudsman are responsible for the development and implementation of information security policy in Finland.

The Ministry of Economy, Trade and Industry of Japan and the National Police Agency hold regular seminars with non-governmental organizations to provide users with information on how to protect themselves from computer viruses and unauthorized access to information. Meanwhile, the security portal of the National Police Agency provides online security lectures and technical consultations for the Internet users.

Norway and Spain also have websites to raise public awareness of information security. The site, created in Norway, offers courses for people from different walks of life (business people, seniors, schoolchildren, teachers, parents, etc.).

Furthermore, recommendations are published on the Internet regarding the methods for privacy protection (accounts, personal data, photos) on how to behave in social networks and chats, safe shopping in online stores, choosing valid passwords, ensuring the security of information exchange, protection against viruses, cyber attacks, and how to protect against Trojans and spyware.

In Spain, the Association of Internet Users conducts information campaigns on information security. Websites and portals are created for the public to provide various information on information security issues. One of those websites is developed by the “Computer Security and Virus Initial Information Center”, that provides the Internet users with detailed information about viruses and current warnings. The site also provides general information about computer security, software security updates, expert advice and discussion forums.

Many developed countries take measures to raise the level of information security of small and medium-sized businesses on information security:

- Preparation of guidelines and recommendations on security for small and medium businesses;
- Organization of seminars on information security issues;
- Development of websites and portals;

- Establishment of a resource center on computer security for small businesses;
- Implementation of electronic competences in business and administration;
- etc.

The member states of the Organization for Economic Co-operation and Development also carry out various awareness-raising and advocacy activities in education for the formation of CIS for students, teachers, parents and adolescents.

4. Measures for establishment of culture of information security in education

Ensuring the safety of children and adolescents on the Internet, the most vulnerable group of the population, is the focus of both countries and international organizations. Several important steps have been taken in this direction in the EU, one of which was the Safer Internet Program adopted in 1999 [15]. The goal of the program was to combat illegal content and destructive behavior on the network and to ensure the safety of children and adolescents by raising their awareness. The main areas for the implementation of the "Safe Internet" Program were:

- financing projects aimed at creating a safe online environment for children and adolescents;
- supporting Safe Internet Day;
- organizing Safe Internet Forum;
- supporting and stimulating corporate self-regulation;
- cooperation with other international organizations.

The "Safe Internet" program has been implemented in stages since 1999 (1999–2004; 2005–2008; 2009–2013, etc.).

Three types of Safe Internet Centers (SICs) have been established in EU countries to raise awareness of safe Internet use among citizens throughout Europe, including children and adolescents:

- Awareness centers – those disseminate information materials, hold meetings with children, parents, educators and teachers to raise awareness about the potential online risks that children may face and ways to ensure their safety on the Internet;
- Helplines to provide individual consultations for children, parents and teachers on the provision of security in the network;
- Hotlines to receive information in illegal content detected on the Internet.

The "Insafe" European Network of Safe Internet Centers, which includes information centers and helplines, has been established to coordinate the activities of SICs in the field of information security in European countries [15]. They meet several times a year to share their experiences, as well as exchange information and resources. The network works with schools, families and other relevant organizations to promote the importance of developing collaboration between home and school to ensure safe use of the Internet. One of the important issues is the division of responsibilities between the government, teachers, parents, the media and other institutions involved in protecting the rights and needs of citizens, especially children and youth.

As children and young people are born in the age of modern technology compared to older generations, they master technical skills more easily and do not have difficulty in mastering technology. Therefore, the Information Centers use the knowledge, skills and potential of young people to inform about information security in a more effective way. Members of the youth panel that currently operates within the framework of the Information Centers inform their peers and adults about ways to protect themselves from Internet threats, organize meetings with leaders of national Internet networks in their countries and discuss how to make their services useful and interesting for young people. They also select and recommend useful, interesting, and intellectual resources, and produce a variety of videos, comics, and textbooks on the pros and cons of the Internet.

The Safe Internet Program has been renamed as Better Internet for Kids since 2014. [16]

Many countries are already training cybersecurity specialists from school desks. Thus, in Israeli schools, children learn to program at grade 4. Successful students in this subject are offered additional classes in cryptography and cyber-security at certification centers.

Cybersecurity competitions are held once a year among young people in England. Under British law, school staff are required to be trained in security issues each year, including Internet security. Together with SWGfL, a leading organization in child safety on the Internet, which supports new educational technologies in the country, SIC conducts a wide range of e-safety trainings for schools and other organizations working with children and youth across the country.

The 360 Degree Safe program developed by SWGfL allows schools to evaluate their own network security measures, compare them with others, prioritize the areas where improvement is needed, and, at the same time, receive advice and support to move forward.

In Australia, blockchain and cryptoalgorithms have been taught since 2018 in the primary school. This allows children to receive digital education, as well as bridge the digital divide between children and adults.

The US National Security Agency organizes summer camps for students, schoolchildren and even kindergarten teachers. The practice of creating so-called "white hackers" groups, including students who are well versed in information technology, is widely used. These teams test the software for various vulnerabilities. CTF (Capture the flag) team competitions on information security and system administration are organized to improve the skills of information security specialists.

The International Cyber Sport Federation was established in the Republic of Korea in 2008 and is now very popular in many countries around the world. Competitions in computer sports are held for both professional and amateur athletes, as well as students and pupils. In addition, many educational institutions offer computer science training programs in the field of gaming technology. Ahlman Vocational College of Finland (Orivesi) organizes education in three areas: "technologies of development of computer games", "computer game design", and "cyber sport" [18].

In 2021, the SIC of Greece developed new digital materials for each level of education. The package "Back to School" is available on the SIC's website and is aimed at everyone, from young children to high school students, parents and educators. With the help of these materials, an attempt is made to inform high school students about the language of hate on the Internet, which has recently become widespread. Through various activities, students are taught to recognize the language of hatred and how to react to it when encountered. This year, special attention is paid to informing students about cybercrime: how to protect them from fraudsters and how they should react when faced with this situation. Through interactive presentations and quizzes, learners study about viruses and how to protect themselves from them, such as using secure passwords, determining if an email or information is dangerous, and how to protect against phishing. Even young children are taught the rules of proper use of the Internet with the help of fairy-tale characters.

The Portuguese National Cyber Security Centre organizes large-scale open online courses for employees working in all fields, including education. In 2019, a course "Citizens in Cyber Security" was developed [16]. It instils "cyber-hygiene" recommendations and practical skills for ordinary workers in various sectors of the economy, and are involved by over 30,000 citizens in the first year. Based on the opinions, wishes and notes of the course participants, misinformation, online shopping and safe use of social networks were included in the course program.

The 2017 Cyber Security Event in Brussels [20] calls on EU countries to make a commitment to include cybersecurity in their academic and professional training programs. It states the necessity to strengthen the critical thinking of children and youth, increase their level of media literacy so that they can adequately respond to threats, cyber threats, cyber security threats and fraud in the content of false information.

The document states that cybersecurity education should not be limited to IT specialists, but should be included in the curriculum in engineering, business management, law and other areas. Finally, teachers and high school students need to be educated on cybercrime and cybersecurity. Since 95% of incidents are intentional or unintentional, cybersecurity is the responsibility of every human

5. Conclusion

It is very important to achieve the comprehensive development of the information society, the transition to the digital economy, as well as the development of CIS in society to ensure the information security of both government and commercial enterprises and citizens.

International organizations and individual countries take measures to increase and develop the level of societal CIS in several directions: increasing the competence of specialists in information security and its assessment; raising the level of awareness of government employees, small and medium business representatives in the field of information security; raising the level of awareness of citizens, including the elderly; apprising children and youth, teachers and parents about information security risks and methods of protection in the education system, as well as the norms of ethical behavior, etc..

The analysis of foreign experience and various cybercrimes on the Internet in our country (cyberbullying, dissemination of fake information, seizure of information on bank cards of citizens, blackmail with videos, insulting people on social networks, etc.) provided a ground to conclude that the solution to this problem is to create a system for educating citizens on safe behavior skills on the

Internet. At the same time, this training should be continuous and cover all levels of education, from kindergartens to higher education institutions.

References

1. Okere I., Van Niekerk J.F., Carroll M. (2012). Assessing information security culture: A critical analysis of current approaches. Information Security for South Africa, October 2012, (pp.1—8). https://doi.org/10.1109/ISSA.2012..6320442
2. Alvarez-Dionisi, L. E., Urrego-Baquero, N. (2019). Implementing a Cybersecurity Culture. ISACA Journal, 2., 1-7.
3. Corradini I., Nardelli E. (2020). Social Engineering and the Value of Data: The Need of Specific Awareness Programs. International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity, (pp.59—65). https://doi.org/10.1007/978-3-030-20488-4_6
4. Mahmudova R.Sh. (2021). About some aspects of the culture of information security of the individual and society. Problems of the information society (in Azerbaijani), 1, 56-66. https://doi.org/10.25045/jpis.v12.il.05
5. Petrenko, S.A., Petrenko, A.A. (2015). Cyber-learning: ENISA guidelines. Cybersecurity issues: scientific and practical journal (in Azerbaijani), 3 (11), 2-14.
6. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. https://www.oecd.org/sti/ieconomy/15582260.pdf
7. Sladkova, N.M., Ilchenko, O.A., Stepanenko, A.A., Shaposhnikov, V.A. (2021). Features of assessment of competences in information security of public municipal services. Issues of state and municipal management (in Russian), 1, 122-149.
8. Official website of the EU Cyber Security Agency. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity/@@download/fullReport
9. Dvinskikh, D.Yu., Talapina, E.V. (2019). Risks of development of data turnover in public administration. Issues of state and municipal management (in Russian), 3, 7–30.
10. Competency Model for Cybersecurity (2011). https://www.chcoc.gov/content/competency-model-cybersecurity
11. National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
12. Secure Trust Bank PLC Annual Report & Accounts 2020. https://www.securetrustbank.com/images/InvestorRelations/r2020/STB-Pillar-3-Annual-Disclosures-2020-Final.pdf
13. Joint Communication of the European Commission and European External Action Service: Re-silience, Deterrence and Defence: Building strong cybersecurity for the EU. https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-europe
14. Malyuk, A.A., Polyanskaya, O.Yu. (2016). Foreign experience in the formation of information security culture in society. Information technology security (in Russian), 4, 25-37.
15. Cybersecurity&Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas
16. Safer Internet Programme: Emprowering and Protecting Children Online. Europe's Information Society. http://ec.europa.eu/ information_society/activities/sip/index_en.htm
17. EU "Better Internet for Kids" Programme. https://www.betterinternetforkids.eu/en-GB/home
18. Website of an organization ensureing safety of children on the Internet in the UK. https://swgfl.org.uk/
19. Official website of Ahlman College, Finland. https://www.ahlman.fi/
20. Official website of the Greek Center for Safe Internet. https://www.betterinternetforkids.eu/en-GB/sic/greece