Information security of the personality of the subjects of the educational process

Irena Robert[1,*], *Viktor* Polyakov[1], and *Oleg* Kozlov[1]

[1]Institute of Education Management of the Russian Academy of Education, 105062, 5/16, 1B, Makarenko str., Moscow, Russia

Abstract. The article is devoted to the training of specialists in the field of information security of the personality of participants in the educational process. The theoretical and practical bases of training and promising directions of fundamental and applied scientific research in this field are substantiated and described. The work was carried out within the framework of the State task for the Program of Fundamental Scientific Research of the State Academies of Sciences for 2013-2020 (in the part of RAO) (approved by the Decree of the Government of the Russian Federation of December 3, 2012 No. 2237-r) within the theme "Development of the Informatization of Education in the Context information security of the person" (the state registration No 14.07.00.20.01.04).

1 Introduction

The current stage in the development of the information society of global mass network communication, both in our country and abroad, is characterized by a large-scale introduction of information and communication technologies (ICT) in all significant spheres of life (e-government, e-learning, "learning management," electronic commerce, Internet and mobile banking, telemedicine, social networks, electronic publications, intellectual property, presented in electronic form, and others). The flip side of these processes is the emergence of new risk factors and threats to information security for the individual, society and the state. In this case, the information security of the subjects of the educational process, which use the means of ICT in their work, is of particular importance.

Significant changes in the system of legal provision of information security applied to the system of domestic education have occurred over the past few years. For the education sphere, the important role is played by the Federal Law of December 29, 2010, No. 436-FZ "On protecting children from information that is harmful to their health and development," which introduces the concept of information security for children. The requirements of this law were reflected and further developed in the National Strategy for Children for 2012-2017 (approved by Presidential Decree No. 761 of June 1, 2012), which states that the level of development of high technologies achieved today, the country's openness the global community led to the problem of insecurity of children from illegal content in the

[*] Corresponding author: rena_robert@mail.ru

information and telecommunications network of the Internet, exacerbated the problems associated with trafficking in children, child pornography and prostitution. " As one of the objectives of the strategy, it is proposed to introduce a system of scientific and monitoring research on the security of the information and educational environment of educational institutions.

Further development of the policy of the Russian state in the field of ensuring the information security of the individual was developed in the National Security Strategy of the Russian Federation (Decree of the President of the Russian Federation No. 683 of December 31, 2015 "On the National Security Strategy"), which notes that an ever increasing influence on the character of the international situation has an increasing confrontation in the global information space, conditioned by the desire of some countries to use information and communication ion technology to achieve its geopolitical objectives, including through the manipulation of public consciousness and the falsification of history ... There are new forms of illegal activities, in particular with the use of information, communication and high technologies. To ensure national interests, science, technology and education are listed as strategic national priorities.

The set of official views on the goals, objectives, principles and main directions of ensuring information security in the Russian Federation is presented in the new Doctrine of Information Security of the Russian Federation (Decree of the President of the Russian Federation No. 646 of December 5, 2016 "On Approving the Doctrine of Information Security of the Russian Federation"), which represents a system of official views on ensuring the national security of the Russian Federation in the information sphere.

Further impetus in the state building of the information society in our country was given in the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030 [Presidential Decree No. 203 of May 9, 2017 "On the Strategy for the Information Society Development in the Russian Federation for 2017-2030"], which is the basis for determining the goals, objectives and measures of the domestic and foreign policy of the Russian Federation in the field of application of information and communication technologies for the development of the information society of the global mass a marketing communications network, the formation of a national digital economy, realization of national interests and strategic national priorities, certain National Security Strategy of the Russian Federation.

2 Methods

In the Doctrine of Information Security of the Russian Federation [Doctrine of Information Security of the Russian Federation (approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646) is envisaged as the development of personnel potential in the field of ensuring information security and application of information technologies, as well as ensuring the protection of citizens against information threats, including by creating a culture of personal information security. The provisions of the Doctrine, as well as other components of the legal and organizational support of the information security of the individual, should be the basis for training specialists of any profile in the field of personal information security. In addition, the training of specialists in the field of information security of the individual must be determined by all levels of vocational education: secondary, higher, postgraduate, additional and focused on various areas of training and specialties.

The theoretical basis for training specialists in the field of personal information security is research in the field of multi-level training (Robert, I. V., Vagramenko, Y. A., Vostroknutov, I. E., Kozlov, O. A., Lavina, T. A., Lapenok, M. V., Martirosyan, L. P., Mukhametzyanov, I. Sh., Serdyukov, V. I., Shikhnabieva, T. Sh., etc.), adequate to civil education, based on information law and information culture (Beshenkov, S. A., Kozlov, O., Mindzaeva, E. V., Polyakov, V. P.).

The practical part of the training of specialists in the field of personal information security is aimed at the formation of strong information security skills in the development of educational, methodological and organizational support, the correct use in the information systems and networks (local and global Internet) of general and special software.

3 Research

The foregoing determines the need for future specialists to develop knowledge in the following areas:

- the essence, importance, relevance and peculiarities of the problem of ensuring the information security of an individual with regard to implementation in the sphere of education, in legal, organizational, economic and financial management systems, in information systems and ICT, in the basic concepts in this subject area;
- peculiarities of information and information systems as an object of protection, the main threats to information resources in the sphere of education, legal, organizational, economic and financial management systems, possible consequences of the impact of threats and ways of their implementation;
- bases of legal maintenance of information security of the person and information protection in information systems;
- principles and content of organizational support of information security of information systems;
- methods and means of hardware and software information security in information systems;
- the criteria for the protection of information systems and the principles of building an integrated information security system;
- bases of computer virology, methods and means of protection of information systems from computer viruses and malicious programs;
- requirements for users of information systems and recommendations for ensuring their information security;
- the basis for the protection of information and information constituting state and commercial secrets.

As a specialist, a future specialist needs:

- as a user, to assess the nature of information security threats in the information system in use;
- effectively use available methods and tools to ensure information security of modern computer systems;
- practically implement general rules and measures to ensure information security in the information system used.

The future specialist in the field of personal information security should have strong skills:

- protection of electronic documents and their fragments (texts, tables, databases, etc.) from accidental or deliberate changes using the basic capabilities of the Windows operating system (Linux) and Microsoft Office suite (Open Office);
- use digital signatures and certificates to protect electronic documents;
- archiving and reservation of documents;
- work with specialized anti-virus tools - on checking computer facilities for the presence of computer viruses, their neutralization and removal, updating of the anti-virus database;

- collective work and protection of information in local computer networks and the global Internet;
- work with technical literature on issues of information security, access delimitation and information protection.

Selection of the training content of a specialist in the field of personal information security is carried out according to the following parameters:

- correction of the content of the training material on the information security of the individual with a view to its compliance with the relevant Federal State Standards for Higher and Secondary Vocational Education;
- cooperation of all departments and structures of the university on the basis of integration of opportunities for access to information resources, equality and sovereignty;
- development and experimental approbation of curricula and programs with subsequent corrections;
- application of various technologies of interaction, including alternatives to traditional methods and techniques to develop creativity in activities, increase motivation.

In this regard, for any profile of training specialists using the means of ICT in educational and future professional activities, it is advisable to include the professionally oriented discipline "Personal Information Security" in the curricula of the curriculum studied, the main purpose of which is the formation of competence in the field of personal protection from:

- external aggressive information of the party: the media; Internet advertising of goods, services and illegal activities and activities prohibited by law; Internet-communities or network associations that impart a certain opinion; social networks that form a collective opinion;
- unethical information that offends the moral values and feelings of the user, from: Internet portals that allow unethical expressions, or information that offends the moral values and feelings of the user; Internet portals, aimed at obtaining personal data of the user without his knowledge; Internet communities that provide on-line communication with an anonymous subject, the purpose of communication with which can be criminal.
- poor-quality pedagogical products implemented on the basis of information and communication technologies that do not meet the pedagogical-ergonomic requirements, from: Internet advertising, Internet portals, firms offering educational products (non-licensed organizations) (electronic educational resource, various methodologies and methodological recommendations) and educational services (training, psychological trainings, etc.);
- loss of copyright for intellectual property, presented in electronic form, from: Internet publications, publishing and replicating electronic publications, electronic educational resource, without indicating the source; private websites, web pages, replicating information obtained at random, without specifying the source; sites of educational institutions that publish current educational materials without reference to the authors.
- deliberately manipulating the consciousness of a person performing certain actions with information, including in networks, and/or participating in the realization of plots of Virtual Reality systems, presented by audio-video clips in computer games, in private communication with the user (s), including in social networks);
- the relationship between modern people, due to the possibility of an easy replacement of a partner by a "cyber partner" in various forms of communication on the Internet or by facilitated communication without problems.

In connection with the foregoing, scientific and methodological approaches to certification of software and hardware, educational information complexes, methodology and technology of formation of evaluation indicators of pedagogical products realized on the basis of ICT have been developed to form pedagogical-ergonomic, medical-psychological, technological assessment groups. Theoretical models for assessing the quality of pedagogical products implemented on the basis of ICT have been developed on the basis of expert and statistical methods of assessing compliance with the requirements of international standards on safety and quality. Technical conditions for expertise and certification of pedagogical products, functioning on the basis of ICT are also developed: electronic editions for educational purposes; electronic means of educational purpose; applied software and automation systems for information and methodological support of the educational process and management of the educational institution; educational and methodological complexes, including electronic editions for educational purposes and electronic educational tools; information networks of an educational institution; distributed information resource for educational purposes of local and global networks; educational laboratory equipment matched with a computer; automated workplaces of the user (employee of the educational institution). Methodological recommendations on the use of indicators of pedagogical-ergonomic and medico-psychological quality of pedagogical products, implemented on the basis of ICT, were also developed.

Thus, the content of the professionally-oriented academic discipline (or course) “Information security of the individual” is focused on the formation of a complex of knowledge about the current state of the problem of ensuring the information security of the individual, the existing threats and types of information security, the fundamentals of building information security systems, as well as the ability to apply methods and means to protect their information sphere from external negative impact and protection from external influences personal information. In its turn, the methodologically substantive part of the discipline has a system-forming character and is aimed at forming competencies ensuring a conscious perception by the user of modern ICTs of all complexity and responsibility of the information security problems of an individual, understanding the difficulties in securing it, the associated tight constraints and large material costs, and skills in ensuring information security in the face of tough competition.

As a result of studying the discipline, students should know:

- the essence of the problem of ensuring the information security of the individual and the features applicable to the sphere of future activity, its importance and relevance, the basic concepts in this subject area;
- characteristic features of information and information systems as an object of protection, the main threats to information resources in the sphere of future activity;
- the basis of legal support for the information security of the individual (elements of the information law, aspects of information security in the system of national and economic security of Russia, constitutional norms, laws of the Russian Federation and Decrees of the President of the Russian Federation, responsibility for computer crimes);
- principles and content of organizational support of personal information security (security policy, control, delineation and restriction of access to information resources);
- methods and means to ensure the information security of the individual (authentication and identification of users and technical means, organization of information protection in personal computers, cryptographic transformation of information and electronic signature);
- features of ensuring information security in databases and in telecommunications networks;
- basics of computer virology, methods and means of protection against computer viruses and malicious programs;
- requirements for ICT users, including those on the Internet, and recommendations for ensuring the information security of the individual.

Particular attention in this case should be given to the formation of skills:

- Work in a network with a digital signature,
- Providing “password protection” of documents,

- Database encryption,
- Practical familiarization with security measures on the Internet, including when working with e-mail, protection against spam,
- The use of modern means of archiving and copying information, as well as anti-virus protection packages.

When preparing in the field of information security, interdisciplinary ties should also be used effectively, establishing a correlation of different disciplines:

- in the field of general humanitarian and socio-economic disciplines - philosophy, sociology, political science, culturology, law (to highlight the role and importance of information and information resources in modern society, including ensuring the rights and freedoms of the individual, the importance of their humanitarian, moral and ethical , culturological, legal aspects);
- in the field of general mathematical and natural science disciplines - mathematics and its applications (to highlight questions about the use of mathematical methods for converting data to protect them).

Here are the aspects of the invariant of training in the field of personal information security in the table.

Table 1. Aspects of the information security invariant in the teaching of students.

Social aspects of information security of the individual	Legal aspects of information security of the individual	Technological aspects of personal information security
1. Information structure of the Russian Federation. 2. Information security and its components. 3. Threats to information security and their classification. 4. Basic types of information. 5. Problems of information security in the world community.	1. Legislative and other legal acts of the Russian Federation regulating legal relations in the sphere of information security of an individual, society, state, and also protection of various types of secrets. 2. The system of security information security in the Russian Federation. 3. Administrative and legal and criminal liability for violations in the information sphere.	1. Protection against unauthorized interference in information processes. 2. Organizational measures, engineering and technical and other methods of protecting information, including information constituting state secrets. 3. Protection of information in networks, anti-virus protection. 4. Specificity of processing confidential information in computer systems.

4 Conclusion

Promising fundamental and applied research is the development of the course “Information security of the individual,” based on the system approach, implementing in the aggregate philosophical, ideological, socio-ethical, pedagogical, technological, medical and psychological, regulatory and technical, organizational and managerial aspects of information security personality. Let us dwell in more detail on their description.

Pedagogical, technological and socio-ethical aspects of the content of training in the field of personal information security are fundamental, since the study of the pedagogical aspects of the information security of the personality of the subjects of the educational process makes it possible to identify the significance of the problem both at the civilizational level and at the personal level in full accordance with the humanitarian component of the information security of Russia. As a result of studying the subject of this block, trainees should know the essence of the problem of ensuring the information security of the individual and its characteristics in relation to various areas of educational and future activity, as well as its importance and relevance. Trainees should be aware of such factors as, firstly, the isolation of the user of ICT from the surrounding real world (due to the user's enthusiasm, both information interaction in networks, and motivated extracted and perceived information); secondly, the stereo- audio-visual representation of the phenomena being studied or explored is based on the “ease” of perception of information, since in this case the user’s visual-figurative thinking is “exploited” and the logical, abstract thinking is weakened; thirdly, the ease of transformation, management and modification of both screen (virtual) objects, and the conditions of their interaction, creates a high emotional background of the information interaction itself. At the same time, when studying a certain subject area, the trainee must know the peculiarities of information systems and information used by him in various areas as an object and subject of protection, he must understand the main threats to information resources in all socially significant areas of human activity, he must know the role of the human factor in solving problems ensuring information security.

It is people who make up the most vulnerable “component” of information resources and pose the greatest danger to them both in the information and educational environment and in the individual use of information and communication technologies. Therefore, among the areas of addressing the problem of personal information security, such as the creation of secure operating systems and applications, the improvement of security equipment, and the improvement of the legislative framework, the education system plays an important role.

At present, the ethical problems of the use of information and communication technologies that arise due to the lack of clarity on the question of what ethical restrictions, both social and personal, must be fully resolved are not fully resolved. The mechanical transfer of the currently existing normative ethical norms and rules in the conditions of the information society of mass network communication becomes inadequate to modern realities.

The technological aspect of training, determines the security conditions and the use of information systems and technologies (the safety of the user's personal data, the legitimacy of the content of information systems and its quality in terms of scientific, ergonomic, etc. indicators). Within the framework of studying the technological aspects of ensuring the information security of an individual when using information and communication technologies, including information systems for applied and instrumental purposes used for educational purposes and in the sphere of future activity, the following should become the subject of study: the principles and content of organizational information security, control, delineation and restriction of access to information resources); principles for the creation of comprehensive information security systems; methods and means of ensuring information security (authentication and identification of users and technical means, organization of information protection in personal computers, cryptographic transformation of information and electronic signature); features of information security in databases and telecommunications networks; basics of computer virology, methods and means of protection against computer viruses and malicious programs; requirements to users of information and communication technologies and recommendations for ensuring personal information security). At the same time, the selection of content and its structuring should ensure that trainees understand the fact that, despite the abundance of dangers and threats, it is possible to maintain the necessary and sufficient level of information security and minimize risks associated with the organization, investment and level of user training.

An obligatory component of training in the information security of the individual is to study the basics of its legal provision. Among the tasks to be solved by the state in the sphere of ensuring the information security of an individual is the intensive development of legal regulation of relations in the field of countering threats, priority interests in the information sphere are consolidated, which is facilitated by the adoption of a significant number of legislative acts. Law enforcement practice in the field of combating unlawful acts against freedom, honour and dignity of a person, constitutional rights and freedoms of a person and citizen, realized in the information sphere, is steadily growing. These circumstances predetermine the obligation to study the basics of legal support for the information security of the individual, the content of which should be the understanding of the complexities of legal regulation of relations in the information sphere, conditioned by the very notion of "information," the lack of unity of its interpretation in jurisprudence. In this context, the aspects of the person's information security in the system of national and economic security of Russia, the relevant constitutional norms and legal acts, responsibility for computer offenses, as well as the levels of legal regulation and the system of state bodies in the field of information security should be studied. The study of the legal aspects of the information security of the individual should be aimed at eliminating legal nihilism, a conscious perception of all those restrictions that exist due to the existence of state, banking, commercial, professional, official, personal secrets and copyright.

One of the important directions in the development of the training of specialists is the development of the activity component of the content, i.e. inclusion in the minimum required content of the education of specially selected methods of activity, techniques and technologies, key competencies and other procedural elements that the learner needs to master. In the formation of competence (the experience of applying theoretical knowledge, skills and skills to solve problems in the subject area), the relevant workshops should become the mandatory conditions for training specialists in the field of personal information security. In such workshops, as a means of training pedagogical and management personnel, it is proposed to include network tools for the development of an electronic educational resource, the content of which assumes the implementation of the "embedded" capabilities of information technologies (computing, search, analytical, model-forming).

References

1. S. A. Beshenkov, E. V. Mindzayeva, Remote and Virtual Training, **5** (2016)
2. O. A. Kozlov, M. I. Bocharov, Scientists Notes IIO RAO, **43** (2012)
3. O. A. Kozlov, A. A. Malyuk, Informatics and Education, **10** (2013)
4. I. Sh. Mukhametzyanov, *Methodological recommendations on prevention of negative medical consequences of the use of ICT in education* (IIO RAO, Moscow, 2012)
5. V. P. Polyakov, Global scientific potential, **4**, 13 (2012)
6. V. P. Polyakov, *Youth extremism: the origins, warning, and prevention: proceedings of the international scientific-practical conference (May 23-24, 2014)* (MPSU, Moscow, 2014)
7. V. P. Polyakov, *Materials of the scientific-practical conference 22-23.04.2011.* (MODEK, Moscow, 2011)
8. Russian Academy of Education, *Recommendations for reviewing electronic editions of educational purposes. used in the educational process of educational institutions of the initial general. basic general. general secondary education* (IIO RAO, Moscow, 2013)

9. I. V. Robert, *Theory and Methods of Informatization of Education (Psychological, Pedagogical and Technological Aspects)* (BINOM: Knowledge Laboratory, Moscow, 2014)
10. I. V. Robert, Pedagogical Informatics, **2** (2017)
11. I. V. Robert, Pedagogy, **10** (2015)
12. Russian Academy of Education, *Sistema voluntary certification (SDS) of hardware-software and information complexes for educational purposes (APIKON)* (IIO RAO, Moscow, 2013)
13. *Explanatory dictionary of terms of the conceptual apparatus of informatization of education* (BINOM: Knowledge Laboratory, Moscow)