Current security issues in the information society

Anastasia Filippova[1*]

[1] Kikot Moscow University of the Ministry of Internal Affairs of Russia, Russian Federation, 117437, Moscow, st. Academician Volgina, 12., e-mail fipovaa@mail.ru

Abstract. That scientific research highlights specific items of modernization in the field of public society information security. Taking into account professional and public orientation, government support is aimed at promotion of human recourse, provision of information support. Currently human mind is one the most valuable item. In this regard, jurists are responsible for explanation of political, economic and legal points. Moreover, it is rather important to reveal an experienced specialist in it. Among the new challenges and threats, the problem of information security is the main one. Information technologies cause considerable impact on management of humans being. Scientific analysis of problems in the field of information security has shown that there is an insufficient level of public awareness. More precisely the problem is in ability to use password with high degree of protection, spread of unnecessary information in social networks. In that research are touched upon various concepts of information society. Also, main theories and elements are analyzed, which are included into meaning of information society. The difference between main information and other types of social values are covered. Specifics of the above problem, its reasons and impact on development of society are outlined. The conclusion encompasses problems of legal regulation of information security (fragmentation, absence of system). In cognitive activity, scientific complex, including legal, economic, scientific and practical approaches was used.

1 Introduction

Information exists in all spheres and aspects of life. Information is something that occurs in mind, as a reaction (to hear/see), that generates consciousness. Information is unalive process. Security issues in the information society are multilateral, which has been many times drawn attention both in Russian legal science [1], civil science [2], [3], [4], [5], [6], [7], [8] as well as in foreign science [9], [10], [11]. Moreover, the article analyzes Russia's conceptual and doctrinal approaches of international information security ensuring, as well as Russia's initiatives in international organizations (United Nations, BRICS, and Organization for security Co-operation to Europe). For the first time, the term "information" appeared in the 16th and 17th centuries and was translated as an explanation. In the 20-30s, the term was interpreted as a tool for consciousness. Now, there are different approaches to understanding "information": humanitarian, cybernetic, mathematical, philosophical, and attributive. The most significant types are: reactive (to respond adequately), resource (accumulation on resources), background (the most subtle adaptation mechanisms, on properties of which hidden coding technologies are built). Creation of cyber viruses, cyber terrorism, and cybercriminals can destroy the structure of any state.

Society sticks with a massive informational impact on digital sovereignty. In other words, there are interventions in national and internal affairs, provoking inter-ethnic and inter-religious strife.

We must protect ourselves. We must produce immunity. Currently information technology allows to occupy foreign country peacefully. Therefore, in the Russian Federation has been developed a national security strategy that considers these factors. In that, strategy is set the following task: to counteract, thus not to be affected by impacts of information flows that exist in TV, social networks, business cannot work without a computer.

Crime is both destructive and constructive. Law enforcement agencies considered that it deserves to make "prevention" of healthy state, healthy relationships. Thus, law enforcement agencies should train a specialist for practical activities using a competence-based approach (reactive vector). Accordingly, there should be a clear model of a specialist with skills and functions, for example, if there are programs that violate someone's copyright, then you can close the domain itself and the server.

The absence of necessary information is caused by the unsystematic data security, inadequate coordination of state measures to protect information, departmental disunity in sphere of preservation of information, and lack of control over the export of Russian scientific technologies, weapons, and management. Measures for the protection of state secrets, commercial and official secrets in state authorities and management and in defense enterprises have been seriously weakened. Also,

* Corresponding author: fipovaa@mail.ru

protection of personal data, tax, customs, and property information is poorly organized.

The lag of Russian information technologies is caused by purchases of import equipment that cannot resist cyber threat, which increases the possibility of unauthorized access to databases and data banks, and also increases the dependence of the Russian Federation on foreign manufacturers of computer and telecommunications equipment and information products.

2 Problem Statement

The situation with information security in the Russian Federation is such that it does not allow to join the world information system on an equal basis and requires urgent solutions from law enforcement agencies to solve the following key problems:

1. to improve the legal and regulatory framework to ensure information security, including development of registry of information resources, the regulation on information exchange for law enforcement authorities, regulatory, consolidation responsibility of officials and citizens for observing requirements of information security;
2. develop mechanisms and devices for the implementation of citizens' rights for information;
3. arrange information security systems that are an integral part of the country's overall national security system;
4. develop advanced methods and technical tools that provide a comprehensive solution to information security problems;
5. develop criteria and methods for evaluating the effectiveness of information security systems and tools and their certification;
6. to study the forms and methods of civilized influence of the state on the formation of public consciousness;
7. implement a comprehensive approach to the activities of information systems personnel, including methods to increase motivation, moral and psychological stability and social security of people working with secret and confidential information.

Based on the provisions, law enforcement agencies to ensure information security must carry out all measures to protect information in the political, economic, defense and other areas of state activity. Each sphere of state activity requires a special organization of law enforcement agencies. It has its characteristics, this is due to the nature of solving the tasks set, the presence of weak elements and vulnerable links related to in each area of information security.

3 Research Questions

An implementation of information technologies into its modern circulation sets new interdisciplinary tasks for national and world science, which can be solved by conducting research on various legal phenomena, including identifying current problems of ensuring security in the information society.

To achieve the research goal, it is necessary to consistently and systematically resolve a number of issues of a theoretical and practical nature, namely: to analyze the existing domestic and foreign doctrine; to study the legal framework of the issue, identifying a set of problems related to the mechanisms for bringing to justice entities that involved into circulation by means of information systems; to consider the practice of applying existing legal norms in order to identify the range of issues which should be regulated by law, as well as systematize the identified problems and identify ways to solve them.

4 Purpose of the Study

This research is conducted in order to identify issues and their scientific justification related to information protection in society, namely, subjects involved into legal relations using information and communication technologies. The developed scientific positions will become the basis for creating adequate modern legal structures that meet the requirements of the digital economy, and further improvement of legislation.

5 Research Methods

In research the author was based on the following methods: (1) general cognition methods (dialectic, systemic approach), which allowed to consider actual problems of security of the information society as a unified system of legal norms; (2) general scientific methods (analysis and synthesis, system-functional, analogies, modeling), which allowed to establish individual elements of information security, to identify General patterns of information protection in society, (3) special legal (comparative legal, legal forecasting), which allowed to identify formal and logical connections, to formulate prospects for ensuring security in the information society.

6 Findings

In scientific literature, numerous sources are devoted to security issues in the information society, in domestic literature: L. Karsavin, A. F. Losev, V. N. Muravyov, in foreign: K. Knorr-Cetin, J. URR, E. Giddens, and A. Toffler.

Problems identified in particular scientific literature can be divided into several groups: problems related to general methodological support of information security; problems related to ensuring technological independence; problems related to scientific and educational support for continuous training in the field of information security. Thus, there is a necessity to study the theory of object-centered sociality, the sociology of mobility, and the theory of postmodernity.

According to regulatory legal acts, to ensure information security, law enforcement agencies must take all measures to protect information in the political, economic, defense and other areas of the state. Each sphere of state activity requires a special organization of law enforcement agencies, they have their own characteristics, this follows from: the nature of solving the tasks set, the presence of weak elements and sensitive links involved in each area of information security.

According to research by the analytical, center [12], in Russia, in 2020 year the number of informational leaks increased by 46% in comparison with 2018 year. Another analytical, center [13] predicts that by 2021, the volume of (informational) - leaks will increase by 66%. In 2019 year, informational leaks from Russian companies and government agencies amounted to 395 cases, which is 15.7 % of the global number of leaks. The most common cases are: 76.7% - leakage of payment information and personal data, among them – 72.1%, when employees of organizations are found guilty and 4.6% - when management is responsible for. Russia, for the seventh year, ranks second after the United States in the list of countries most severely affected by informational leaks.

According to the Internet Security Alliance, problems, which the information society is collide with, are caused by leakage of personal data, cyber warfare, terrorism and commercial espionage. Thus, there is a task for an expert to improve artificial intelligence and related products, in addition to adequately and effectively use machine learning to prevent, detect and predict attacks.

Each problem has a solution in its area, so the recommendations by Information technology Alliance on Internet security suggest modernize research in the field of information technology and digital programs, adapting cooperation between the public and private sectors, and introducing new methods of investigation in the field of computer power [14].

For example, the interactive Contour BI platform of Contour Components companies [15] provides access to corporate data, the advantages of which are expressed in highly productive Analytics, publication of statistics and data security (for example, customers of the software industry in the United States are – Decision technology, Inc.Software Spectrum; in Germany – Focus DV-Technologies' GmdH.; in Italy – FinWin Srl.). These interactive reports and data analysis are used by thousands of organizations in more than 70 countries in the following industries: public sector, healthcare, consulting, mass media, education, software, industry, statistics, etc.

7 Conclusion

The review of current problems of ensuring security of information society leads to the conclusion that content needs to be filtered considerably, and monitoring of information resources in particular should be conducted. Of course, the work on ensuring security in the information society includes the implementation of goals and objectives that are indicated in the document "Economic security Strategy of the Russian Federation for the period up to 2030", as well as in documents of international organizations.

To achieve efficiency in the legal regulation of information security issues, it is necessary to:

- develop a register of information resources necessary for the exchange of information for law enforcement agencies,
- establish the responsibility of officials and citizens for information security requirements compliance;
- structure the information security system, which is an integral part of the overall national security system of the country;
- develop methods for evaluating the effectiveness of information security systems and tools and their certification;
- develop a system of regulatory support in order to train personnel in the field of information security;
- perform new social mobility as a measure of security;
- improve methods, special and educational literature in the field of creation of effective mechanisms for the use of information technologies in the educational sphere, including technological support for training personnel in the field of information security;
- analyze the problems of information security related to the influence of the Internet on the consciousness of the subject (public).

Currently, the potential of negotiations on security issues in the information society is not exhausted, this is due to objective factors that create necessary basis for the subsequent development of a global document on information security.

References

1. V. N. Lopatin, Information law, 14 – 19 (2018)
2. A. A. Vnukov, *Fundamentals of information security: information protection: textbook for secondary professional education,* 161 (Yurayt, Moscow, 2020)
3. V. V. Gafner, *Information security: a textbook*, 324 (Phoenix, Moscow, 2017)
4. S. V. Zapechnikov, N. G. Miloslavskaya, A. I. Tolstoy, D.V. Ushakov, *Information security of open systems. Means of protection in networks*, 558 (Hotline – Telecom, Moscow, 2018)
5. A.V. Ivanov, Evaluation of information Security against leakage through channels of side electromagnetic radiation and interference, 64 (Liters, Novosibirsk, 2019)

6. A.V. Krutskikh, *International information security: theory and practice*, 384 (Aspect Press, Moscow, 2019)
7. O.V. Koshko, E.M. Romanova, *Economics and management: problems and solutions,* 37 – 47 (Moscow, 2019)
8. R.V. Meshcheryakov, A.A. Shelupanov, *SPIIRAS Proceedings* **3(34)**,136 – 159 (2014)
9. M. Walker, *CEH Certified Ethical Hacker All-in-One Exam Guide*, 1092 (McGraw-Hill Education, 2016)
10. S. Winterfeld, J. Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Syngress, 2012)
11. A. Toffler, *The third wave*, 544 (Morrow, New York, 1980)
12. Information security software products and solutions, URL: https://www.infowatch.ru/analytics/reports (date of access: 01.12.2020)
13. Accenture, URL: https://www.accenture.com/ru-ru (date of access: 01.12.2020)
14. T. Stonier, *Information wealth: a profile of the post-industrial economy*, 393, 395 – 396 (Thames Methuen, London, 1983)
15. Contour BI, URL: https://www.contourcomponents.com/ru (date of access: 01.12.2020)