

## IV. CRIMINAL LAW AND PROCEDURE

**Information for citation:**

*Efremova M. A. Sotsial'naya obuslovlennost' ugovorno-pravovoy okhrany informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Social Conditionality of Criminal Law Protection of Information Security in the Russian Federation]. *Vestnik Permskogo Universiteta. Juridicheskie Nauki – Perm University Herald. Juridical Sciences*. 2017. Issue 36. Pp. 222–230. (In Russ.). DOI: 10.17072/1995-4190-2017-36-222-230.

UDC 343.45

DOI: 10.17072/1995-4190-2017-36-222-230

***SOCIAL CONDITIONALITY OF CRIMINAL LAW PROTECTION  
OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION***

**M. A. Efremova**

Kazan Law Institution (branch) of the Academy of the Prosecutor General's Office of the Russian Federation  
41, Moskovskaya st., Kazan, 420021, Russia

ResearcherID: E-6250-2016

ORCID: 0000-0001-6037-6921

Articles in DB "Scopus" / "Web of Science":

DOI: 10.14505/jarle.v7.1(15).11

e-mail: seamaid63@gmail.com

**Introduction:** information security is one of the components of the national security of the Russian Federation. Recently, the role of the information component of national security has increased significantly. There are new challenges and threats to the information security of the Russian Federation that require reaction of the legislator. Criminal legislation needs modernization to improve its efficiency in terms of criminal law protection of information security. This is evidenced by a combination of factors that determine the need to strengthen the criminal law protection of information security. **Purpose:** to study the factors that necessitate the strengthening of criminal law protection of information security. **Methods:** the methodological framework of the research is based on a set of scientific methods, including general scientific methods (materialist dialectic) and specific scientific ones (systemic-structural, comparative law and others). **Results:** at present, criminal law protection of information security of the Russian Federation does not meet the modern realities. Socio-economic, historical, political, socio-legal and criminological factors indicate the necessity of adopting legislative measures. **Conclusions:** regulations of the Criminal Code of the Russian Federation on criminal law protection of information security require improvement.

---

Keywords: information; information security; computer information; information protection; criminal law

**Information in Russian**

***СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ***

**М. А. Ефремова**

Кандидат юридических наук, доцент, профессор кафедры  
основ организации и управления в органах прокуратуры  
Казанский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации  
420021, Россия, г. Казань, ул. Московская, 41

ResearcherID: E-6250-2016

ORCID: 0000-0001-6037-6921

Статьи в БД «Scopus» / «Web of Science»:

DOI: 10.14505/jarle.v7.1(15).11

e-mail: seamaid63@gmail.com

**Введение:** одной из составляющих национальной безопасности Российской Федерации является информационная безопасность. В последнее время роль информационной составляющей национальной безопасности существенно возросла. Появились новые вызовы и угрозы информационной безопасности Российской Федерации, которые требуют реакции законодателя. Уголовное законодательство нуждается в модернизации с целью усиления его эффективности в части уголовно-правовой охраны информационной безопасности. Об этом свидетельствует совокупность факторов, которые обуславливают необходимость усиления уголовно-правовой охраны информационной безопасности. **Цель:** исследовать совокупность факторов, обуславливающих усиление уголовно-правовой охраны информационной безопасности. **Методы:** методологическую основу исследования составляет совокупность методов научного познания: общенаучные методы (материалистической диалектики), частнонаучные методы (системно-структурный, сравнительно-правовой и др.). **Результаты:** уголовно-правовая охрана информационной безопасности Российской Федерации в настоящее время не отвечает современным реалиям. Социально-экономический, исторический, политический, социально-правовой и криминологический факторы свидетельствуют о необходимости принятия законодательных мер. **Выводы:** нормы УК РФ, направленные на уголовно-правовую охрану информационной безопасности, нуждаются в совершенствовании.

Ключевые слова: информация; информационная безопасность; компьютерная информация; защита информации; уголовный закон

### Introduction

The new version of the Russian Federation's National Security Strategy<sup>1</sup> has information security issues included in nearly all its sections concerned with the achievement of strategic national priorities. This means a close relation between national security and security in the area of information. This is also where the duality of information security reveals itself. On the one hand, it is a part of national security, and as such it acts as an element in a complex multi-level system comprised of various types of security and aimed at achieving such a degree of protection of the Person, the Society and the State from internal and external threats which ensures the exercise of constitutional rights and freedoms of Russian citizens, decent quality and standard of living, sovereignty, independence, national and territorial integrity, and sus-

tainable socio-economic development of the Russian Federation. The provisions outlined in the Strategy were further developed in the new version of the Doctrine of Information Security of the Russian Federation<sup>2</sup>. This document not only assesses the current state of information security in the Russian Federation, but also identifies a list of threats, as well as a set of tools that can provide the required level of protection of the information security in the Russian Federation. In the document, legal means of ensuring information security are assigned to the priority area of activity.

Speaking about the legal tools to ensure information security, it should be noted that the potential of criminal law means has been used to the least extent. However, information security should be viewed as an object of criminal law protection. In this capacity, it presents itself as an open dynamic

<sup>1</sup> National Security Strategy of the Russian Federation, approved by the Decree of the President of the Russian Federation of December 31, 2015 No. 683. Available at: <http://kremlin.ru/acts/news/51129> (accessed 20.03.2016).

<sup>2</sup> 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. Available at: <http://www.scrf.gov.ru/security/information/document5/> (accessed 20.03.2016).

system of social relations which ensure that interests of the Person, the Society and the State in the area of information are met. Meanwhile, the provisions which are concerned with criminal law protection of information security are located in different sections and chapters of the Russian Criminal Code, which hardly satisfies the intensive rates of the information technology development. Criminal law should reflect changes in crimes against information security. Therefore, information security as a social value needs to be reframed, and reasonable criminal law measures need to be taken in response to any infringements. The social conditionality of the rules of law should be treated as the prerequisite of their effectiveness. Despite the fact that rules of criminal law, much like standards in all other branches of law, are enshrined in the national legislation as a result of a conscious human activity, their origins, however, should be sought in the laws of social development. The ultimate foundation of criminal law protection is the social need for protection of a certain group of social relations [11, pp. 46–48]. Therefore, the nature of criminal law, first of all, comes down to the objective laws of social development, when the need for protection of social relations which became especially important and valuable to the society at a particular point in time arises.

The concept of social conditionality is rather broad and comprises a number of intrinsic factors which together act as indicators of the need for modification of criminal law. In our view, the factors which determine the need to distinguish information security as an object of criminal law protection should include socio-economic, historical, political and socio-legal factors.

#### **Socio-Economic Background of Information Security Protection by Criminal Law**

The role of socio-economic conditionality of law rules is fundamental and driving. “Correspondence between juridical laws and the laws of economic development of the society is the most important prerequisite to their effectiveness.” [8, p. 101]. In this regard, it appears reasonable to give a detailed review to this factor first of all.

Socio-economic background of criminal law protection of information security is principally

determined by the fact that the Russian Federation is now entering a new post-industrial stage of development – the so-called “information society” era. The development of the information society in Russia requires reframing of the hierarchy of social relations protected by criminal law. The term “information society” was introduced at nearly the same time by the U.S. economist Fritz Machlup, who was studying the information sector of the economy by the example of the U.S., and by Yujiro Hayashi, a professor at Tokyo Institute of Technology, who used this term in reports submitted to Japanese government by the Economic Planning Agency, Japan Computer Usage Development Institute and Industrial Structure Council. In those reports, information society was defined as the society where the development of computer technology can help secure access to reliable sources of information for its members and provide a high level of industrial automation.

The concept of the post-industrial information society was developed by a number of Western sociologists, including D. Bell, J. Galbraith, J. Martin, I. Masuda, F. Polak, E. Toffler. In Russia, the concept of the information society was studied by V. Glushkov, N. Moiseyev, A. Rakitov, A. Sokolov, A. Ursul and others.

It should not be left unmentioned that many leading world powers have already entered the stage of the information society, and a number of legal instruments governing the information society development have been adopted internationally [13, 17]. For example, Okinawa Charter on Global Information Society, which was signed by the leaders of the G8 countries on July 22, 2000. The Charter is, first of all, a call for everyone engaged in both governmental and private sectors of the economy to fill the international gap in the area of information and knowledge. The Charter promulgates the promotion and encouragement both of transition to the information society and of the implementation of all its economic, social and cultural benefits as the foremost objective. At the World Summit on the Information Society (WSIS) held in Geneva in 2003, Declaration of Principles “Building the Information Society: a Global Challenge in the New Millennium” was adopted, and in May 2005 –

Declaration of the Committee of Ministers on Human Rights and the Rule of Law in the Information Society<sup>1</sup>.

For the Russian Federation, the fundamental document in this area is the Strategy for the Information Society Development<sup>2</sup>. The Strategy incorporates and accommodates fundamental provisions of the Okinawa Charter on the Global Information Society, Declaration of Principles “Building the Information Society”, Plan of Action of the Tunis Commitment and other international instruments adopted by the WSIS.

According to the Strategy, the purpose of building and developing the information society in the Russian Federation is to secure higher quality of living to its citizens, provide Russia with a competitive edge, develop the society in economic, socio-political, cultural and spiritual areas, and also to improve the public administration system through the use of information technology.

An information society is characterized by an increasingly important role of the information sphere, which is understood as a “combination of information, information infrastructure, subjects engaged in collection, compilation, dissemination and use of information, and also a system for regulating the emerging social relations related with information and information infrastructure as objects of interests of the Individual, the Society and the State” [9, p. 56]. It is obvious that the phenomenon of information is the core element of the information sphere and, accordingly, of all information processes which occur in the society [5, p. 28].

According to the scientific community, distinctive features and characteristics of the information society are:

- development of the information and telecommunications technology market;
- reliance of the economy on the level of the development of information and telecommunications technology in a particular country;
- mass use of computers having access to information and telecommunications networks, and the ability of the public to operate such computers;

– ability to search and retrieve information freely from information resources, and also to disseminate and share information through information and telecommunications networks;

– enhancement of requirements for information security to protect interests of the Person, the Society and the State in the information sphere [3, p. 22; 6, pp. 95–100].

The ultimate point of the information society evolutionary development in a particular state is the integration into the global information society. Distinctive features of the latter are:

– being formed as a result of a social revolution which is of the global nature and which is based on the intensive development and convergence of information and telecommunications technologies;

– a prerequisite to well-being of both an individual person and a particular state is knowledge which has been obtained due to the availability of free access to information and the ability to handle such information;

– the process of information exchange is boundless;

– cross-cultural interaction and the emergence of new opportunities for implementation at the same time [7, p. 161].

In 2013, Russia was rated 40<sup>th</sup> according to the ICT development index [14]. The index value is derived from 11 indicators characterizing the penetration of fixed telephony, mobile communications and the Internet (including broadband access), access to computers and to the Internet for households, the level of information skills possessed by adults, and the involvement of the youth in the education process. Russia’s rating according to the Index is one of the performance benchmarks for the Strategy for the Information Society Development in the Russian Federation and for the National Program “Information Society (2011–2020)”<sup>3</sup>. The performance benchmarks are provided in the attachment to the Strategy, and their achievement should confirm the rates of the information society development in the Russian Federation. Both the Strategy and the Program shall be implemented in several phases. The phases are delineated

<sup>1</sup> Declaration of the Committee of Ministers on Human Rights and the Rule of Law in the Information Society: Document CM(2005)56 final 13.05.2005. Available at: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805da1a0](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0) (accessed 15.02.2016).

<sup>2</sup> Strategy for the Information Society Development in the Russian Federation, approved by the Decree of the President of the Russian Federation of February 7, 2008 No. Pr-212. *Rosyskaya Gazeta* – Russian Gazette. 2008. 16 February. No. 34.

<sup>3</sup> Resolution of the Government of the Russian Federation of April 15, 2014 No. 313 “On the Approval of the National Program “Information Society (2011–2020)”. Collection of Legislative Acts of the Russian Federation. 2014. Issue 18 (Pt. II). Art. 2159.

because of the need to sum up the results of implementation of the Strategy and to update the information society development objectives. In implementation of the innovation scenario, the Program not only deals with the tasks in the field of information technology but also becomes a tool for achievement of modernization objectives in other spheres (management, education, health and others), regional development and integration into the world economy, increasing the quality of human capital and the living standard. A 10-times growth in the amount of communications services (2.6 times by 2015 with reference to 2010, and 2.7 times over the period of implementation of the second phase of the Program in 2015–2020) and more than 2-times growth in the size of the IT market are predicted by the year 2020. However, as soon as in 2014 and 2015 Russia showed a decline in performance, being rated 42<sup>nd</sup> and 45<sup>th</sup>, accordingly.

Meanwhile, the Russian Federation has already established an adequate framework for the formation and development of the information society. The very Strategy for the Information Society Development in the Russian Federation mentions that an increase in added value in the economy shall be achieved mainly through intellectual activity, technology level growth in the industry and wide introduction of the latest information and telecommunications technologies. Economic systems are gradually integrated into the knowledge-driven economy, where intellectual production factors act as the driving force.

Since modern scientific and technological advances – including latest information and telecommunications technologies – can be and are already used for criminal purposes [12, 15, 16], provision of security in the sphere of information is a prerequisite to the successful formation of the information society in Russia. And the more developed the information society is, the more resources and equipment the State will need to ensure its security. The law with all its intrinsic methods shall have the leading role in the national security framework that is being created.

Thus, the bottom line is that the socio-economic factor of conditionality of information security criminal law protection is related with the development of a new type of society in Russia where information and communications technologies are of paramount importance. The country's economic development also depends on these technologies as Russia transits

from a petro-state to an information-based and knowledge-driven economy. The spiritual and social needs of people are now concerned with the rapid lookup of relevant information, obtaining timely, complete and reliable information and being able to exchange such information.

### **Historical Background of Information Security Protection by Criminal Law**

The next factor – historical conditionality of information security protection by criminal law – involves the evolutionary development of legislation in this direction. As already mentioned hereinabove, the provisions which are concerned with criminal law protection of information security are located in different sections and chapters of the Russian Criminal Code. Chapter 28, Crimes in the Sphere of Computer Information, was included in the Criminal Code of the Russian Federation in 1996, and later, in 2011, it saw fundamental changes as all its three articles were restated. The need for amendments to be made to provisions of Chapter 28 of Russia's Criminal Code was long highlighted in literature, which would actually be done 15 years after enactment of the current Criminal Code. Information technology development rates call for changes in legislation. Criminal law should reflect changes in crimes against information security. Therefore, the next step should be to reframe information security as a social value, and reasonable criminal law measures need to be taken in response to any infringements.

### **Political Background of Information Security Protection by Criminal Law**

The political factor is related with the political challenges the Russian Federation is currently facing, both internal and external. In accordance with the Art. 4 of Federal Law "On Security"<sup>1</sup>, the Government's security policy, which is essentially an integrated set of coordinated political, institutional, socio-economic, military, legal, information, special and other measures joined by common intent, is an integral part of the Russian Federation's internal policy. New challenges and threats to Russia's national security have arisen recently, which are reflected by the new National Security Strategy of the Russian Federation

<sup>1</sup> Federal Law of December 12, 2010 No. 390-FZ "On Security". Collection of Legislative Acts of the Russian Federation. 2011. Issue 1. Art. 2.

approved by the Decree of the President of the Russian Federation of 31.12.2015 No. 683. As mentioned in the document, whereas the Russian Federation pursues independent internal and foreign policy and goals, it is facing opposition from the United States and their allies, who put political, economic, military and informational pressure on the country. The Strategy stresses that aggravation of confrontation in the information space caused by the desire of certain states to employ information and communication technologies in the achievement of their geopolitical goals, including by way of manipulation with public opinion and perversion of history, has been increasingly impacting the international atmosphere. New forms of illegal activities are emerging, in particular, those using information, communication and high technologies. Among other threats to national and public security, the document mentions the activity involving the use of information and communication technologies for spreading and propaganda of fascism, extremism, terrorism and separatism ideology, undermining national accord and political and public stability in the society. The Strategy names the improvement of statutory regulation of crime control, including in the information sphere, among key areas of national and public security, for which purpose the system for identification and analysis of threats in the sphere of information followed by appropriate response measures is being improved. In other words, information security issues are embedded in nearly all chapters of legislation which are concerned with the realization of strategic national priorities, making it possible to conclude that the role of information security in the national security system is being reframed.

#### **Socio-Legal Background of Information Security Protection by Criminal Law**

And last, but not least, the socio-legal factor. As already mentioned above, the war on crime in the information sphere is one of the major areas of national and public security efforts, which is undoubtedly related with the increased public danger of offenses in the information sphere. The information sphere, despite its significance, is one of the

least protected spheres and, as such, it is vulnerable to various forms of illegal activity. Provisions protecting information security that are scattered across the Russian Criminal Code cannot serve as an effective tool to combat crimes in the information sphere.

There is a reoccurring trend towards the increase in a number of computer crimes currently observed in Russia, and those crimes are just a part of a total number of crimes against information security. This fact is demonstrably evidenced by historical data as well. For example, there were 2,698 crimes in the sphere of computer information on record in 2011, 2,820 crimes in 2012, 2,563 in 2013, 1,739 in 2014, and 2,382 in 2015. After some decline in 2015, a growth in crimes in the sphere of computer information is being observed again. At the same time, in 2015 in Russia damages from such crimes, according to estimates by some experts, amounted to \$1 billion. Others claim that the amount of such damages is even greater. Crimes in the sphere of computer information are characterized by a high degree of latency, and as such official statistics would hardly reflect the real picture.

U. Zinina reasonably notes that the actual computer crime clearance data in Russia is distorted as a result of the frequent misapplication of rules of Chapter 28 of the Russian Criminal Code in investigative and judicial practice, in part because of expansive interpretation of elements of offenses addressed by that Chapter and misunderstanding of technical fundamentals [2, p. 13]. Therefore, official statistics that show a decline in computer information crimes may indicate the inadequate effectiveness of rules of Chapter 28 of the Russian Criminal Code, high latency of this class of crimes and the need for drastic measures to be taken.

#### **Results**

Before any conclusions can be drawn, we should concur with N. Kuznetsova and G. Zlobin that between a social need and its reflection in criminal law there is a historically formed social consciousness of a given historical period that determines the nature, forms, and degree of accuracy of legal reflections. Rules of law, unlike objective laws of nature, may be “good” or “bad”, i.e. they may either appropriately reflect a social need or be

insufficiently relevant to that need, achieve or not achieve goals set by the legislator [4, p. 76]. Provisions of the Russian Criminal Code that address criminal law protection of information security scarcely reflect the actual social need for its protection by criminal law. Having become a new value, a basis of living and a driver of trade and industry development, the Information requires the State to focus its efforts on creating the appropriate environment to ensure its security. The social circumstances that have developed bespeak the need to recognize information security as an independent object of criminal law protection.

Underestimation of criminal law measures within the legal mechanism of ensuring information security endangers interests of the Person, the Society and the State in the information sphere. A. Ter-Akopov stresses that the information threats that have emerged require a more thorough scientifically-based consideration. Criminal law plays a special role here, as it has to generalize socially dangerous manifestations of offenses against information security of the Person, the Society and the State [10, p. 165].

The most urgent threats to information security existing at the current stage include:

- development, creation, and use of any means that are intended to impact and damage information resources and telecommunications systems of the State;

- purposeful information influence on critical entities;

- information influence aimed at disruption of political, economic and social systems of states, and brainwashing of the public to cause destabilization of society;

- unauthorized interference with information and telecommunications systems and information resources, as well as their improper use;

- activities of international terrorist, extremist and criminal associations, organizations, groups and individual offenders that pose a threat to information resources and critical entities of the State;

- the use of information technology and facilities to the prejudice of basic human rights and freedoms that are exercised in the information sphere;

- cross-border dissemination of information that is contrary to guidelines and rules of the International Law, as well as to national legislation of the affected states [7, pp. 242–249].

Russia's information security policy distinguishes the following types of threats to the national information security according to their nature:

- threats to the constitutional rights and freedoms of the human and citizen with regard to spiritual life and information activities, to individual, group and social consciousness, and to Russia's spiritual renovation;

- threats to information support of national policy of the Russian Federation;

- threats to development of the national information industry, including IT, computerization and communications industry, to meeting the domestic market needs for the industry's products and their entry to the international market, as well as to the accumulation, integrity and effective use of national information resources;

- threats to the security of information and telecommunications facilities and systems, both already deployed and in progress of creation within Russia.

The above threats reflect the downside of IT development and are far from fiction, they are quite real. New threats are predicted as well, necessitating "proactive institutionalization" [1] of criminal law standards concerning information security protection, which should be based on a common criteria.

## Conclusions

Therefore, social conditionality of information security protection by criminal law is determined by a number of interrelated socio-economic, historical, political and socio-legal factors. The said factors act as prerequisites to the criminalization of acts against information security. Those factors are unique because they are all associated with the process of formation and development of the information society in the Russian Federation, and they attest to the need for extension of the list of information offenses that are forbidden by law.

## References

1. Zhuk M. S. *Puti sovershenstvovaniya sistemy institutov rossiyskogo ugolovnogo prava* [Ways for the Improvement of the System of Institutions of the Russian Criminal Law]. *LEX RUSSICA*. 2015. Issue 4. Pp. 46–59. (In Russ.).
2. Zinina U. V. *Prestupleniya v sfere komp'yuternoy informatsii v rossiyskom i zarubeznom ugolovnom prave: avtoref. dis. ... kand. jurid. nauk* [Crimes in the Sphere of Computer Information in Russian and Foreign Criminal Law: Synopsis of Cand. jurid. sci. diss]. Moscow, 2007. 33 p. (In Russ.).
3. Kopylov V. A. *Informatsionnoe pravo* [Information Law]. Moscow, 2004. 510 p. (In Russ.).

4. *Kuznetsova N. F., Zlobin G. A. Sotsial'naya obuslovlennost' ugolovnogo zakona i nauchnoe obespechenie normotvorchestva*. [The Social Conditionality of the Criminal Law and Scientific Support for Rule-Making]. *Sovetskoe gosudarstvo i pravo – Soviet State and Law*. 1976. Issue 8. Pp. 76–83. (In Russ.).
5. *Kunyaev N. N. Pravovoe obespechenie natsional'nykh interesov Rossiyskoy Federatsii v informatsionnoy sfere: dis. ... d-ra jurid. nauk* [The Legal Support for the National Interests of the Russian Federation in the Information Sphere: Dr. jurid. sci. diss]. Moscow, 2010. 420 p. (In Russ.).
6. *Lopatin V. N. Informatsionnaya bezopasnost' Rossii: dis. d-ra ... jurid. nauk* [Information Security of Russia: Dr. jurid. sci. diss]. St. Petersburg, 2000. 433 p. (In Russ.).
7. *Polyakova T. A. Pravovoe obespechenie informatsionnoy bezopasnosti pri postroenii informatsionnogo obshchestva v Rossii: dis. ... d-ra. jurid. nauk* [The Legal Support for Information Security When Developing Information Society in Russia: Dr. jurid. sci. diss]. Moscow, 2008. 438 p. (In Russ.).
8. *Redzhepov A. Sotsial'naya obuslovlennost' ugolovno-pravovykh norm kak faktor povysheniya ikh effektivnosti* [The Social Conditionality of Criminal Law Norms as a Factor in Increasing Their Effectiveness]. *Tezisy dokladov na teoreticheskoy konferentsii aspirantov Instituta gosudarstva i prava AN SSSR i juridicheskogo fakul'teta MGU – Abstracts of the Theoretical Conference of Post-Graduate Students of the Institute of State and Law of the USSR Academy of Sciences and the Faculty of Law of the Lomonosov Moscow State University*. Moscow, 1981. Pp. 101–102. (In Russ.).
9. *Strel'tsov A. A. Teoreticheskie i metodologicheskie osnovy pravovogo obespecheniya informatsionnoy bezopasnosti Rossii: dis. ... d-ra jurid. nauk* [Theoretical and Methodological Basiss of the Legal Support for Information Security of Russia: Dr. jurid. sci. diss]. Moscow, 2004. 371 p. (In Russ.).
10. *Ter-Akopov A. A. Bezopasnost' cheloveka. Sotsial'nye i pravovye osnovy* [Human Security. Social and Legal Foundations]. Moscow, 2005. 272 p. (In Russ.).
11. *Filimonov V. D. Norma ugolovnogo prava* [The Rule of Criminal Law]. St. Petersburg, 2004. 198 p. (In Russ.).
12. *Buchan R., Tsagourias N. Cyber War and International Law. Journal of Conflict & Security Law*. 2012. Vol. 17(2). Pp. 183–186. (In Eng.).
13. *Maillard de J., Roche S. Crime and justice in France; Trends Policies and Political Debate. European Journal of Criminology*. 2004. January. Vol. 1. Pp. 111–151. (In Eng.).
14. *Measuring the Information Society*. Available at: <http://d-russia.ru/wp-content/uploads/2013/11/MIS2013.pdf> (accessed 12.01.2016). (In Eng.).
15. *Minott N. The Economic Espionage Act: Is the Law All Bark and no Bite? Information & Communications Technology Law*. 2011. October. Vol. 20. Pp. 201–224. (In Eng.).
16. *Mitrakas A. Information security and law in Europe: Risks checked? Information & Communications Technology Law*. 2006. March. Vol. 15. Pp. 33–53. (In Eng.).
17. *Ryder N., Reid A. S. E-Crime. Information & Communications Technology Law*. 2012. October. Vol. 21. Pp. 203–206. (In Eng.).

#### References in Russian

1. *Жук М. С. Пути совершенствования системы институтов российского уголовного права // Lex Russica*. 2015. № 4. С. 46–59.
2. *Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. ... канд. юрид. наук. М., 2007. 33 с.*
3. *Копылов В. А. Информационное право. М.: Юрист, 2004. 510 с.*
4. *Кузнецова Н. Ф., Злобин Г. А. Социальная обусловленность уголовного закона и научное обеспечение нормотворчества // Советское государство и право*. 1976. № 8. С. 76–83.
5. *Куняев Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: дис. ... д-ра юрид. наук. М., 2010. 420 с.*
6. *Лопатин В. Н. Информационная безопасность России: дис. ... д-ра юрид. наук. СПб., 2000. 433 с.*
7. *Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. ... д-ра юрид. наук. М., 2008. 438 с.*
8. *Реджепов А. Социальная обусловленность уголовно-правовых норм как фактор повышения их эффективности // Тез. докл. на теор. конф. аспирантов Ин-та государства и*

- права АН СССР и юрид. фак. МГУ им. М. В. Ломоносова. М.: Изд-во ИГиП АН СССР, 1981. С. 101–102.
9. *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. ... д-ра юрид. наук. М., 2004. 371 с.
  10. *Тер-Акопов А. А.* Безопасность человека. Социальные и правовые основы. М., 2005. 272 с.
  11. *Филимонов В. Д.* Норма уголовного права. СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2004. 198 с.
  12. *Buchan R., Tsagourias N.* Cyber War and International Law // *Journal of Conflict & Security Law*. 2012. Vol. 17(2). P. 183–186.
  13. *Maillard de J., Roche S.* Crime and justice in France; Trends in Policies and Political Debate // *European Journal of Criminology*. 2004. January. Vol. 1. P. 111–151.
  14. *Measuring the Information Society*. URL: <http://d-russia.ru/wp-content/uploads/2013/11/MIS2013.pdf> (дата обращения: 12.01.2016).
  15. *Minott N.* The Economic Espionage Act: Is the Law All Bark and no Bite? // *Information & Communications Technology Law*. 2011. October. Vol. 20. P. 201–224.
  16. *Mitrakas A.* Information security and law in Europe: Risks checked? // *Information & Communications Technology Law*. 2006. March. Vol. 15. P. 33–53.
  17. *Ryder N., Reid A. S.* E-Crime // *Information & Communications Technology Law*. 2012. October. Vol. 21. P. 203–206.