

## National Information Security in Russian Federation and Abroad

*Alexander A. Galushkin*

Department of Judicial Authority, Law-Enforcement and Human Rights Activity of the Peoples' Friendship University of Russia 117198, Russia, Moscow, Miklukho-Maklaya str. 6

---

**Abstract:** In the present article author discuss organizational and legal questions in the field of information security and its defense on the governmental (national) level. In past 10-20 years with growing informatization and active computerization and globalization questions of national information security started to play a key role and became a part of national security strategies of many developed countries. Nowadays it is clear that without good national information security strategy and appropriate reasonable measures on its practical implementation it's impossible to think of good level of stability and security in the country. Unlike centuries before, nowadays bulk amounts of information can be send through Internet with one simple click. It became much easier as well to publish data and be sure that it would be seen by many people almost instantly. Due for this and many other reasons modern information technologies are widely being used by criminals, terrorists and for the espionage. In the conclusion of the article author presents personal ideas on some positive changes in the field of national information security of Russian Federation.

**Key words:** Information • Information technologies • IT • Security • Cyberterrorism • Crime • Counteractions • Practice • Problems • Globalization • Russia • Russian Federation

---

### INTRODUCTION

Modern level of science and technology allow quick transfer of bulk amounts of information locally or worldwide [1] through information telecommunication networks (including the Internet) and communication channels. For this is no longer bulky or unique equipment is required as it was few decades ago. Nowadays usually standard equipment which is in mass production and a civil turn is enough.

With active informatization of civil society, private persons and organizations staff started active use and publish personal and proprietary information (including secret, restricted, or other classified information) in the information telecommunication networks (of open, or restricted access) and send it using different information telecommunications networks and communication channels.

It is possible to judge on the popularity of these methods of information distribution by a large number of end users (connections to information telecommunication networks of open and/or limited access) and by quantity of network resources and its popularity.

Until the end of the XX century the best method of mass information distribution was obviously mass media (television, radio, newspapers, magazines, etc. as well as other mass media). However, with mass implementation of general access information telecommunication networks, especially the most popular – Internet, popular Internet resources (web-sites) became true mass medias through which information can be effectively given to readers (users). This is especially interesting because many Internet users go not read paper magazines and newspapers, or even watch TV or listen radio.

Due to the variety of reasons results of active informatization and computerization was particularly significant in countries of former Soviet Union (USSR).

---

**Corresponding Author:** Alexander A. Galushkin, Department of Judicial Authority, Law-Enforcement and Human Rights Activity of the Peoples' Friendship University of Russia; Research Associate at the Moscow State University of Psychology and Education; Research Professor at the International Institute of Informatization and Public Administration named in the honor of P.A. Stolypin.  
Cell: +7 (916) 254-6662.

During communist authority in USSR soviet citizens were cut from most benefits of technological revolution. Personal computers were unknown to most citizens, chances of getting access to Internet were equal to null, special internal scientific and military networks existed.

**Research Methodology:** In the present article authors present summary of conducted research, where research problem was formulated, a good empirical base accumulate, an opportunity to focus on the research process and to draw conclusions that would reflect the real situation in the best possible way using: introduction – hypothesis, deduction – predictions, observation – nest of predictions, etc. was given.

## RESULTS AND DISCUSSION

In the 1990<sup>th</sup> many significant changes in social, economic and political spheres occurred in our country. Collapse of Soviet Union led to many critical changes in civil society role and structure. Foreign products, technologies and services (many of which was not previously available in USSR, or the circle of persons who used those during Soviet Union existence was considerably limited) appeared on Russian market. Personal computers and software for them, as well as printers, scanners and other related equipment for both civilian and military use appeared in Russia and became widespread.

Russia, opposed to other countries in the world felt results of the fourth information revolution associated with invention and introduction into production of microprocessors and specialized programming, as well as the advent of personal computers and portable data transmission technologies (including protocols).

Implementation of post-Soviet Russia was also marked by active network spreading and introduction of opening of mass population to international information and telecommunications network – Internet.

Past few decades on informatization and computerization in Russia specifically and globally in the world was marked by emergence of the significant number of popular Internet resources (from news sites, entertainment portals, services, sharing music, movies and other content to chats, forums, social networks, online shopping and so on).

Gradually moving a significant part of trade and services into the network space (Internet) can be considered a global trend. Also an increasing amount of media switched to partial or complete distribution through the Internet.

Russian Federation, as a full-fledge member of the modern international community is no exception to this rule. Each year an increasing percent of popularity in Russian Federation acquires Internet-based technologies. Gradually, Russian citizens are getting used to buy goods and services through a variety of Internet resources and pay for them in the non-cash ways.

Various forums, chat rooms and social networks are getting increasing popularity and even become more popular than traditional methods of communication. Today majority of Russian citizens have access to Internet an home and/or office, personal computers are found in most homes and offices, many citizens own other computerized devices (smartphones, tablets, TVs and set-top boxes).

Such systems as "smart house", "smart office", "smart car" and others similar in nature system, that are connected to the information telecommunication networks and allow remote control of one or other elements of the system remotely are not surprising nowadays. It would be correct to say that such systems are becoming more and more popular in the middle class.

Russian Federation only recently plunged into the information security problems, due to a number of reasons, the main of which can be considered, as has been said, weak information and computerization of our country before the collapse of the USSR and in the first years after it. However active introduction of new information technology has given rise to new challenges. With the introduction of information technology, computerization and the active transfer of data in electronic form storage has become necessary to protect the information stored on electronic (including network) media and transmitted via information telecommunication networks.

Under Article 29 of the Constitution of the Russian Federation "Everyone shall have the right to freely look for, receive, transmit, produce and distribute information by any legal way" [2]. At this level of information technology implementation into the society and life of individual questions of information protection are becoming particularly important. Complexity of modern methods and techniques requires appropriate level of legislators, law enforcement officers and other professionals work.

On one hand it is necessary to protect personal information, including personal data, however modern development of information technology opens some greater problems – protection of state secrets, commercial and industrial secrets, other critically important data (such as held in different state databases and required for appropriate functioning).

End users are usually trying to solve security issues on given object (within their property) [3] whether it is an apartment, house, building, enterprise, institution or organization, regardless of their legal form of organization and activities. Unfortunately, these measures are often ineffective and do not give expected result in full.

Appropriate measures can only reasonably be done at the federal level. Such approach may be called as national information security. Using information telecommunication networks, including Internet illegal actions are constantly occurring. Currently in Criminal Code of the Russian Federation there are articles "Illegal access of computer information" (Article 272), "Creation, use and distribution of malicious computer programs" (Article 273), "Inappropriate use of storage facilities, processing or transmission of computer and information telecommunication networks" (Article 274). Also there are other crimes that can be done using computer and information systems, including fraud, theft, vandalism, slander, treason, espionage, etc.

In many developed countries there are specialized law-enforcement agencies and/or specialized units of law-enforcement focus, involved in the field of information security at the national level (national information security).

Often work of such bodies is accompanied by the work of scientific organizations (research institutes and centers). Such organizations usually specialize on development of new methods, technologies, equipment capable to identify possible threats and if possible to counteract them. Sometimes they also supply statistical data and assist in development on legal norms. For example Committee on National Security Systems (CNSS) Glossary Working Group take efforts on creation and update of the National Information Assurance Glossary [4]. And for example in Slovak Republic the National Strategy for Information Security is developed. "The purpose of this document entitled "National Strategy for Information Security in the Slovak Republic" (hereafter referred to as the "NSIS") is to lay down an information security framework in the Slovak Republic (hereafter referred to as "SR"). With respect to the fact that ensuring information security (the document covers non-classified information only) requires a comprehensive approach, it is necessary to define its basic level, with an option of further upgrading in specific fields. Well-defined information security is important with a focus on the establishment of primary legislative rules in the respective area, as well as with respect to further steps to be taken to address the issue of information security in Slovakia" [5].

In Russian Federation there is no specialized law-enforcement agencies, specialized law-enforcement units exist in the Ministry of Internal Affairs of the Russian Federation and Federal Security Service of the Russian Federation, however their powers and resources are very limited.

Situation with scientific research in the field is much better. There are many research institutions (both private and public) that develop new mechanisms and technologies as well as research legal problems and work in the field of information law, a number of standards is adopted [6]. Unfortunately no current up-to-date law on national information security exist in Russia. "Regulation of information relations on creation of information society requires careful research" [7].

## CONCLUSION

In modern world of informatization and computerization state plays an essential role in the field of information security. This role may be expressed in the complex organizational and legal instruments to ensure safety of important information, appropriate mode of access to it, obstruction of unauthorized transfer, modify, delete, protect the legitimate rights and freedoms, as well as providing efficiency of the national segment of the Internet and etc.

In the current global context, issues of collective information security in the Russian Federation are particularly relevant and their solution is impossible without competent evidence-based approach [8].

On one hand appropriate theoretical foundation (concepts) of the national information security of Russian Federation should be developed and applied. Said concepts should be an integral part of the National Security Strategy of Russian Federation.

On the other hand effective institutional arrangements to ensure national information security of Russian Federation must be done. So it is especially important to make sure that satisfaction by work of judicial authorities exist in the civil society [9], as well as law-enforcement officers. Appropriate up-to date education of law-enforcement officers, investigators and judges is required.

Unfortunately at the present time, a significant part of the organizational and legal issues of national information security of the Russian Federation are not well worked out.

Also there is no one centralized driving force and author finds it very important to concentrate efforts federally and assist scientific organizations in their researches and what is even more important in implementation of research results. Unfortunately current practice shows that most research results are not being applied to practice for long periods of time or even at all.

It is important to remember that "an ideal civil society is open, democratic, social market society where there is no place for personal authority, a totalitarian modes, violence over people and where full respect of law and morals exist, principles of humanity and justice are exercised by every person" [10].

### REFERENCES

1. Walls Colin, 2005. *Embedded Software*. Newnes, pp: 344.
2. *Constitution of the Russian Federation. Text. Comments.*, Jurcompany, 2013. pp: 24.
3. Itiuridze L.A., 2013. Policy of Access to Information Management // *Pravovaya Initsiativa*, 8: 13.
4. *National Information Assurance (IA) Glossary*, Committee on National Security Systems, 2010. pp: 2.
5. *National Strategy for Information Security in the Slovak Republic*, European Union Agency for Network and Information Security, 2013.
6. *National Standard of the Russian Federation "Information Technology. Practical Rules of Information Security Management."* // Konsultant Plus, 2013.
7. Chesnokov, N.A., 2013. Legal bases of information security in modern conditions // *Pravovaya Initsiativa*, 4: 4.
8. Belov, O.N., 2012. Century of Information Technologies – Century of Information Law // *Pravozashitnik*, 3: 71.
8. Sangadzhiev, B.V., N.N. Marchuk and A.A. Galushkin, 2013. Questions of Fair Justice and Judicial Authority Functioning in Russian Federation // *World Applied Sciences Journal*, 28(7): 920.
9. Grudtsina, L.J. and A.A. Galushkin, 2013. Questions of Modern Civil Society Development in Russian Federation // *World Applied Sciences Journal*, 25(5): 790.