European Proceedings of
Social and Behavioural Sciences
EpSBS
www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.02.02.5

NININS 2020

International Scientific Forum «National Interest, National Identity and National Security»

CONCEPT OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION: WAYS OF IMPLEMENTATION

Vadim A. Adaev (a)*, Kiril A. Maksimov (b), Timur A. Zharov (c)
*Corresponding author

(a) St. Petersburg state University, 7–9, Universitetskaya Embankment, St. Petersburg, 199034, Russia, vadim.adaev@bk.ru
(b) St. Petersburg state University, 7–9, Universitetskaya Embankment, St. Petersburg, 199034, Russia, kamaksimov1410@gmail.com
(c) St. Petersburg state University, 7–9, Universitetskaya Embankment, St. Petersburg, 199034, Russia, catratcatt@gmail.com&

Abstract

The article reflects the basis of the Concept of Information Security of the Russian Federation and its main aspects. Based on the analysis of the current state of information security goals, objectives and issues of information security are defined. Besides, objects, threats of information security and their possible consequences, methods and means of prevention, separation and neutralization of threats, as well as features of ensuring information security in different spheres of activity of the state are considered. The main provisions of State information security policy in the Russian Federation are set out. The Concept serves as a methodological basis for developing a set of legal, organizational and methodological documents regulating the activities of representative, executive and judicial authorities of the Russian Federation, the constituent entities of the Russian Federation, local authorities, enterprises, institutions and organizations regardless of their legal form or form of ownership. For the Russian Federation, as for any country of the world community, it is very important to control, develop, improve, update, stabilize and protect the system of information security after all, the future of the whole country depends on it.

Keywords: Digital signature, enciphering, information security, information security, information threat, information war

https://doi.org/10.15405/epsbs.2021.02.02.5
Corresponding Author: Vadim A. Adaev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The current stage of development of Russian society requires changes in the information sphere, which is the activity of information infrastructure, objects that collect, form, disseminate and use information, as well as the system of regulation of public relations. The information sphere today quickly and actively affects the state of political, economic and defense security of the Russian Federation. The national security of the Russian Federation largely depends on ensuring information security, and this dependence is constantly increasing in the process of technological progress and development of society. Information security of the Russian Federation performs a protective function of the national interests of the country in the information sphere by combining the balance of personality, society and state.

Today, the task of ensuring information security, including in Internet networks, is one of the forms of protection against so-called "new forms of aggression" towards the Russian Federation. This is the urgency of this work.

Information security is one of the strategic directions in the current military and political situation. Work in this direction is carried out within the framework of providing the armed forces with modern technologies and is aimed at creating Russia's military superiority over potential aggressors. It should be noted that information security contributes to the improvement of the quality of strategic nuclear forces, the development of combat capabilities of the army and navy and is the basis for the development of a new type of armed forces – the Military and Space Forces (Fisher, 2014).

Information aggression is used together with political and economic pressure. Thus, "combat information" and information security occupy an important place in modern struggle.

In the conditions of the existing information warfare the Russian government should be ready for any, even the most unexpected, sanctions decisions by the "unpredictable" USA and EU. Western countries have already thought about disconnecting Russians from the Internet because of constant hacker attacks on its part. Although Russia has not done anything like that. NATO representatives have repeatedly announced attempts to break into their websites and steal special purpose information from Russian domains.

IT specialists understand very well who the chief administrator of the global Internet network is. Due to the fact that it is almost impossible to predict the behavior of Western partners, and there is no reason to expect anything good, we must be ready to disconnect Russia from the Internet. Thus, the possibility of creating an autonomous network "Runet" can be considered one of the steps in the field of national information security.

It is no longer a secret that Russian operators have a mechanism to disconnect Russia from the Internet, in case of emergency. If we recall the riots in Egypt in 2011, local authorities have disconnected the Internet and mobile networks throughout the country. Now Russian specialists from the Federal Communications Agency are able not only to disconnect the Internet, but also to administer domains on their own territory. The Ministry of Communications is already able to provide autonomous operation of Runet, without connecting to the global Internet.

2. Problem Statement

The problem of scientific research in the field of information security is a growing competition between the countries of the world in the main strategic issues, the desire and desire to create and implement higher technologies and systems, to obtain information that can turn over the basic concepts of science and technology, fundamental developments, diplomatic secrets and peculiarities of building international relations, the desire to create more technological weapons: tactical, mass, biological, modified types. All this encourages the Russian Federation to pay increased attention to the issue of security and safety of information, which will help protect the country from external threats and attacks (Zverev, 2014a; 2014b).

Today, in a rapidly changing world, in parallel with the process of creating new gadgets and IT-development, there is a growing need to search for protection systems against hardware vulnerabilities and information leaks. While company executives have come to realize the need to build a truly effective information security system, criminals have firmly established themselves in cyberspace. The brightest example is the market in dark web, where a lot of prohibited goods and services are sold, including hacking utilities and access to which is already cracked and opened to the user. In addition, criminals continue to exploit the illiteracy of users in ensuring their own security (Fisher, 2014).

All of these vulnerabilities and information leaks, the zeroing of bank cards, passport and personal information leaks give rise to serious reflection and new insights into the effectiveness of security systems. It is time to review the old approaches and talk about a new type of information security (Sosnin, 2014).

3. Research Questions

According to the analytical agency Positive Technologies, according to Boris Simis, Deputy General Director for Business Development, in 2019 the planned budgets for information security increased on average by 20 %, i.e., the market grew. However, this is a formal growth: if we evaluate it in terms of money actually spent and earned by market participants, the overall bar practically does not exceed last year's figures. The reason of default on budgets in most cases consists in necessity to pass competitive procedures: the companies simply do not have time to buy those protection means which are planned or necessary for preservation of the information and protection against hacker attacks.

In the last couple of years, it was already noted that the provision of information security began to change and more and more companies come to understand that it is necessary to build such a system of protection, which cannot be broken, but today it is very difficult given the development of artificial intelligence and technology progress. A large proportion of systems are either already compromised or could be compromised and the main objective of any security system is to detect the attacker as quickly as possible and to reduce the window of opportunity for him to do irreparable harm. In this connection there is a growth in demand of the highly intellectual protection frames allowing to solve problems on timely revealing of attacks and incidents. In particular, it is a question of systems of class security information and event management (SIEM), network traffic analysis (NTA), complex antiAPT decisions. At the end of the year, interest in this type of technology has increased almost three times.

Companies that aim to really protect themselves in cyberspace today face a total shortage of personnel (Ibor et al., 2018). There is a lack of specialists who have sufficient level of competence to ensure a high level of ability to detect (i.e., deeply immersed in the specifics of the business of the protected companies, watching the security and attack trends, understanding the latest technologies and their vulnerabilities). We can see that there is an increasing demand for specialists with several competences at once: it may be a combination of knowledge in the field of data science and cyber security, deep industry specifics (say, automated control systems) and information security, etc. Business as a result realizes that it does not have necessary quantity of experts of such level, and usually comes to outsourcing or out staffing, and in rare cases even is compelled to train independently the personnel which is not enough in the market.

The tasks of information security are increasingly reflected in regulators' initiatives: the latest requirements, standards and regulations of the Central Bank, Federal Security Service (FSB), Federal Service for Technical and Export Control (FSTEC) are aimed at practical security.

In particular, in 2019, key changes occurred in legislation on the protection of critical information infrastructure facilities (CII), as well as in the regulations of the Central Bank and the Federal Security Service. The most important in CII are new methodological documents that define the procedure for interaction between CII entities and the NCCI (National Coordination Center for Computer Incidents). In them it is explained, about what incidents to inform, what information to transfer, in what term.

There appeared the concept of the State Security Service – a global system for collecting and exchanging information about computer attacks in Russia, formulated in the orders of the FSB #196, 281,

282. They describe the tools to be used by the SSCOPCA center. In addition, specific requirements to SSCOPCA subjects were published, and these are no longer recommendations, but binding documents. The practice of bringing to justice under Article 274 of the Criminal Code ("Violation of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunication networks") has begun to develop, but so far only with regard to the obvious things: they are punished for attacks on the subjects of FII and for serious violations of job descriptions.

It is also expected that amendments to Act No. 187-FZ will be worked out next year, which will correct ambiguous terms and language. FSTEC methodical documents on analysis of threats in information systems are also under development: we hope that in the coming year they will be approved.

No less interesting changes are expected in the Central Bank's regulatory documents: next year three provisions for payment services will come into force. The main conclusion: from January 1, 2020, financial organizations should use software that has either a FSTEC certificate or a certificate of vulnerability analysis. We do not expect that banking software developers will start to carry out mass certification of their solutions, because of all the certification tests only vulnerability analysis and undeclared capabilities are actually required. This is a traditional service demanded by credit organizations with a high level of maturity, but now it becomes mandatory for all financial organizations. It should be separately noted that the procedure of vulnerability analysis, which is referred to by the regulations of the Central Bank, requires that software developers carry out such analysis independently, within the life cycle of development of their products.

Already today it has stirred up the market of bank services and consumers of bank software have started to order services of security analysis. For self-written software, banks actively order static and dynamic code analysis. If earlier such services were mainly of interest for enthusiasts from financial companies, now all the financial organizations without exception need them.

Already today it has stirred up the market of bank services and consumers of bank software have started to order services of security analysis. For self-written software, banks actively order static and dynamic code analysis. If earlier such services were mainly of interest for enthusiasts from financial companies, now all the financial organizations without exception need them.

Security analysis is rather expensive, there are few performers and you have to compete for them already now. In recent months the demand has grown so dramatically that the supply is not in time. Experts of a large company in the sphere of IS (there are four or five of them on the Russian market) can make 30–50 security analysis in a year, and each bank from the first ten of such applications can have 15–20. And these applications are regularly updated, which requires additional vulnerability checks. If an organization has many applications and often releases updates, it will be more profitable to build a secure development process.

For financial software vendors, passing the vulnerability analysis becomes a competitive advantage. Already now many developers of bank software speak about signing contracts with leading companies in the sphere of IS for work on source code analysis. We expect that within the nearest two-three years building a proven cycle of safe development will become the mainstream for bank software vendors (Mazur, 2014).

To remove uncertainty and vagueness in requirements to security analysis, this year the technical committee of the Central Bank (TC № 122) has developed the project of the methodical document "Profile of protection of the applied software of the automated systems and appendices of the credit organizations and the non-credit financial organizations" where it is written in detail how it is necessary to carry out the analysis of vulnerabilities of appendices. For Russia it is the first experience of the obligatory standard document, such specification was only in certification system. Profile of protection is the obligatory document, it is intended for the open market, and it is necessary to correspond to this document. It is not excluded that other departments will follow the example of the Central Bank.

It is necessary to note also occurrence of the law on "sovereign Internet": it is the first case when the federal law obliges the commercial companies (in this case – communication operators) to carry out cyber trainings. Previously, no one obliged companies to assess in such a form how far the system is capable of countering attackers. Similar requirements to owners of significant FII facilities appeared in FSB regulations (owners of significant FII facilities are required to prepare incident response plans and practice them during exercises). While cyber conductions were previously conducted in organisations with a high level of maturity, they will be conducted in the next two to three years in many companies: these requirements apply to all operators of FII.

4. Purpose of the Study

Identification and study of the main aspects of information security that may affect the integrity of the country and the choice of ways of implementation to prevent possible attacks and external threats from unauthorized access to information data of strategic, global importance for the further development of the country, its integrity and security. Study of the specifics of the existing information security market in order to preserve data integrity, security of financial, banking, technological, global systems of information exchange and processing.

5. Research Methods

The research methodology consists in the analysis of the Information Security Concept and its main priorities, the current position of the information security market in the Russian Federation.

6. Findings

In analysing the above, we can conclude that the increasing complexity of information communication between people, automation of the management of industrial facilities, transport and energy have created new opportunities for targeted negative impact, which can be carried out by both unfriendly States, individual groups of criminal orientation or individuals. The realization of such an opportunity is commonly referred to as information terrorism. One qualified hacker is capable of causing damage comparable to a combat operation conducted by a military unit. At the same time, the territorial location of States, which creates natural obstacles to the conduct of traditional operations, is not an advantage in information attacks. The development of information weapons does not require the construction of factories, its establishment by both States and individuals cannot yet be effectively controlled.

Consequently, it is necessary to create a legal and organizational system capable of coordinating the development of our country's information infrastructure in order to prevent or maximize the localization of the consequences of an information war or certain episodes of information weapons use. This must be done without delay.

In accordance with article 20 of the Information Act, the main objectives in the area of information protection are:

- first, to protect Russian citizens from theft and loss of personal information;
- second, to create actions to prevent threats to the security of citizens, society and the state;
- third, to prevent unauthorized actions to change, distort, copy or block information;
- fourth, blocking other forms of illegal interference with information resources and information systems;
- fifth, control over observance of the constitutional rights of citizens to keep personal secret and protection of personal data available in information systems; preservation of state secrets, confidentiality of the documented information in accordance with the legislation.

7. Conclusion

The accumulation of information security problems in various areas reaches its limit. Hardware vulnerabilities have not yet caused damage, but far-sighted companies have begun to include such problems in their threat model now, realizing that when criminals learn how to exploit such vulnerabilities, it will be too late to protect themselves.

APT attacks, on the contrary, have "worked" to their full potential, threatening not only businesses, but also government agencies and infrastructure facilities. News about this year's data leaks has become particularly high-profile, also because cybercriminals have supposedly combined the leaks of past years into a single array for trading in the shadow market with more complete digital user data.

Many technologies have their dark side, which can get out of hand and become a threat to everyone. With the upcoming proliferation of 5G networks, experts link the emergence of new risks for telecom operators. The development of artificial intelligence and machine learning technologies not only makes life more convenient, but also provides a powerful push to improve hacking tools as well as new methods of social engineering.

Comprehensive technology integration generates multiple attack vectors. Confronting threats in an ever-changing world of modern technologies and adapting to the new needs of corporate and private users are top priorities for IS specialists, whose solution may require fundamentally new approaches to cybersecurity.

References

Fisher, J. (2014). *Security of the Post-Soviet Space, New Challenges and Threats International Security in a Multipolar Global Structure with a Special Consideration of the Role of Russia*. Publ. House of the Catholic University of Lublin.

Ibor, E., Oladeji, F. A., & Okunoye, O. B. (2018). A Survey of Cyber Security Approaches for Attack Detection, Prediction, and Prevention. *Int. Journal of Security and Its Application, 12*(4), 15–28.

Mazur, V. (2014). Security of the former Soviet Union, new challenges and threats. *Information Security of Payment Systems* (pp. 373–381). Publ. House of the Catholic University of Lublin. https://clck.ru/MK7fu

Sosnin, A. (2014). Security of the Post-Soviet Region: new Challenges and Threats. *On the protection of information as a multi-vector phenomenon of social development* (pp. 429–438). Publication House of the Catholic University of Lublin. https://clck.ru/MK7fu

Zverev, P. G. (2014a). International peacekeeping in the light of the challenges of international security at the beginning of the XXI century. *Actual probl. of the human. and natural sci., 4*(64).

Zverev, P. G. (2014b). International Security in the Context of Globalization. An article from the coll. of mater. of the V Int. Sci. and Pract. Conf. “Actual Problems of Legal Science: Theory and Practice”, April 14 (pp. 137–138).