Legal aspects of legislative regulation of information security and protection of information in data centers

Elena Golovina[1], *Valentina* Turkova[1], and *Artem* Vasichenko[1,]

[1]Irkutsk National Research Technical University, 664074, Lermontova str., 83, Irkutsk, Russia

Abstract. In modern conditions, information is one of the most important business resources that need protection. Therefore, today, the issue of developing the information security management system and its implementation in organizations is conceptual. The paper reveals the problems of the information security in two main aspects - at the level of legislative regulation and the information security in data centers. A number of features characterizing information as an object of legal relations have been determined. The international standards regulating the issues of information security, in particular the safety of data centers, are singled out. The paper touches upon the main requirements that modern data centers should meet. The authors identified the main types of risks when using an external data center, and suggested ways to minimize them.

1 Introduction

The technology of information storage does not stand still, and is being actively improved from the time of the first rock inscriptions, punched cards, streamers, floppy disks to the creation of a high-performance and fault-tolerant information infrastructure called data centers. In recent years, the computerization of all processes has been particularly intensive. In this regard, information, being at present an extremely capacious concept and embracing all aspects of life, is increasingly associated with the notion of security. All aspects of the security of the individual, society, and the state in turn are increasingly determined by how effectively information, information technologies, information resources, and information interests are protected, and how the society is able to protect itself from harmful information and destructive information influences.

In this article, we will disclose the information security issues in two main aspects:

1. Legislative regulation of the information security, as a concept of capacious and generalizing nature;

2. Ensuring the security of information on such a complex site as a data center that has its own specifics and causes a lot of questions, especially taking into account the large-scale use of the information virtualization and cloud computing technologies in data centers.

By the beginning of the 21st century, information has become an independent driving factor in the evolution of mankind. This circumstance has elevated it to the rank of one of the most effective means of satisfying the conflicting interests of people, which in turn is associated with the emergence and development of all kinds of threats to their rights and

freedoms. Recently, such an integral part of it as the information security of a citizen, society and the state has become very important in the system of ensuring national security of Russia. The Russian information infrastructure created in the interests of all these entities is increasingly becoming a target for various kinds of internal and external threats, often associated with illegal encroachments [1].

The Doctrine of the Information Security of the Russian Federation, which is a set of official views on the objectives, tasks, principles and main directions of providing this activity, prioritizes legal measures to protect information, including protection of intellectual property, which requires further development and improvement [2].

The development of human activity is inconceivable without the exchange of information, its accumulation, systematization, analysis and evaluation. As it is known, there is no a single concept of information in the modern science, thus experts interpret it in different ways. The term "information" originates in the Latin word *informatio* - an explanation, a statement. According to the definition given by S.I. Ozhegov, information means different kinds of messages and data [3].

At one time, K. Shannon introduced the term "information" in a narrow technical sense; with reference to the theory of communication or transmission of codes (this direction is called "Information Theory"). Almost simultaneously with him, Norbert Wiener substantiated the need for an approach to "information" as a general phenomenon that is important for the existence of nature, man and society, as a global phenomenon [4].

Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection" considers it as "information (messages, data) regardless of the form of their presentation" [5, 13].

In a social society, information possesses a special place. In the conditions of real life and relations between people, information reflects the most diverse aspects and forms of their interaction. These relations are of moral, political, national, religious and legal nature. Each public relation is a complex and multifaceted phenomenon that includes elements of different needs of people, accompanied by the appropriate information processes. They are implemented through the use of the appropriate information technologies related to the creation, collection, processing, accumulation, storage, retrieval, dissemination and provision of information. The information processes forming the background for the emergence and realization of all socially significant relations in the society without exception are, of course, of a legal nature, that means the nature of legal relations [6].

Information as an object of legal relations is characterized by a number of features that must be taken into account when forming a policy in the field of its protection, including the legal component of this process.

In most cases, the object of protection is not the information itself in its pure form, but the documented information, that is, fixed on a tangible medium, with details that allow it to be determined by itself or by relevant material carrier. Therefore, its carriers (regardless of the information recorded on them) are considered as additional objects of information protection. They are divided into the following types: a) carriers - sources of information; b) carriers - carriers of information; and c) carriers - recipients of information [6].

As A.I. Alexentsev notes, information security is "preventing unauthorized access to information; creation of conditions restricting the dissemination of information; defending of ownership of possession and disposal of information; prevention of diversion, theft, loss, unauthorized destruction, copying, modification, distortion, blocking, disclosure of information, unauthorized influences on it; preservation of completeness, reliability, integrity, reliability, confidentiality of information, etc." [7].

According to ISO/IEC 17799:2005, information is the asset that, like other important business assets, has a certain value for the institution and therefore needs adequate protection. This is especially important in a business environment. Information security involves

protecting information from a variety of threats to support business continuity, reduce losses, increase profits on the invested capital and expand business opportunities.

Along with the control elements for computers and computer networks, many international standards regulating information protection issues pay great attention to the development of security policy, work with personnel (hiring, training, and dismissal from work), ensuring the continuity of the production process, and to legal requirements.

Turning to international standards, we will see that the ISO 27001 standard defines information security as: "maintaining confidentiality, integrity and accessibility of information; in addition, other properties, such as authenticity, impossibility of refusal of authorship, reliability can be included" [8].

This standard ISO/IEC 27001:2013 "Information technology - Security methods - Information security management systems – Requirements" was developed by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) on the basis of the British standard BS 7799. This standard is a supplement to the standard ISO/IES 17799:2005 "Information technology - Methods of protection - A practical guide for information security management".

The ISO 27001 standard is harmonized with the standards of the quality management systems ISO 9001:2008 [9] and ISO 14001:2004 [10] and is based on their basic principles. Moreover, mandatory ISO 9001 standard procedures are also required by the ISO 27001 standard. The structure of the documentation for ISO 27001 requirements is similar to the structure under ISO 9001 requirements. Most of the documentation required by ISO 27001 could already be developed and could be used within ISO 9001. Thus, if the organization has already got a management system in accordance, for example, with ISO 9001 or ISO 14001, it is preferable to ensure compliance with the requirements of ISO 27001 in the framework of the existing systems.

The introduction and certification for ISO 27001 based on the implemented quality management system according to ISO 9001 implies a significant reduction in the internal costs of the enterprise and the cost of implementation and certification [11].

It should be noted that this is only a small part of the regulatory legal acts that regulate the protection of information, since dispositions of many legal norms in this sphere are of referential or blanket nature and have an indirect effect.

In course of relations connected with the protection of information, there is a transition of potential information accumulated on the appropriate carriers, to the kinetic one, and back. This process is implemented through the implementation of information technologies, which is one more independent group of the objects of information protection.

Data centers are a relatively new phenomenon and are structured to provide complex services in the form of information services, which require increased reliability, both in terms of protecting the territory, and in terms of organizational measures and technical security measures, as well as a high level of security of the information. Data centers are created primarily to increase the productivity of companies that actively use information technology in their activities, as well as to improve the quality of services provided.

There are two major documents that regulate the security of data centers: these are the TIA 942 standard (developed by the association of the US telecommunications industry and primarily touches the organization of the structured cabling systems in the data center and, to a lesser extent, fault tolerance and other engineering subsystems), and classification by levels from the Uptime Institute. Both documents regulate the levels of reliability (Tier).

The ANSI / TIA / EIA-942 standard regulates the requirements for the location of the data centers, the external infrastructure, the telecommunications space inside the data center, the cable system and the cable channels of the data center, and for its infrastructure, depending on the required level of reliability of the data center. Data centers of the Classes I and II may occupy part of some premises, but the Class III and IV objects are to be located

only in separate buildings. In total, the EIA / TIA-942 describes up to 200 different parameters of the data center.

The TIA 942 (Telecommunications Industry Association) standard was developed by the US telecommunications industry association and, first of all, touches the organization of structured cabling systems in the data center and fault tolerance and other engineering subsystems. It has a recommendatory character. The document developed by the Uptime Institute is not a standard, but rather a methodology for standardizing the fault tolerance of a data center. It formulates basic principles of design and approaches. Both a project (Tier Certification of Design Documents), and a working site (Tier Certification of Constructed Facility) and its operation (Operational Sustainability Certification) are certified. Certification is carried out only by the Uptime Institute itself.

There is also a relatively new standard BICSI 002 2010 Data Center Design and Implementation Best Practices, which appeared in 2010 and was updated in 2011. It is designed to supplement existing standards. The European standard EN 50173-5 is also nearing completion, on the basis of which in the future it is planned to form the appropriate Russian GOST [12].

There is specificity in ensuring the complete security of information in data centers. How safe it can be to store data in the data center and how to choose the best data center for the business - these are the main questions that most customers are interested in.

The main function of modern data centers is to increase the reliability of processing and storing information. One of the main criteria for assessing the performance of any data center is the time of availability of the information systems. The data center must ensure business security and minimize downtime risks, meeting the following requirements:

− Fault tolerance. This is a property of the technical system to maintain its operability after the failure of one or more components.
− High accessibility. This property of the system determines its reliability, the ability to perform the required function under specified conditions at a given time or within a specified time interval, provided that a certain set of conditions is met.
− Continuity of business. It includes processes and methods aimed at ensuring non-stop performance of critical business functions.
− Resistance to disasters. This is the ability to recover from a disaster, that is resistance to the impact of accidents and natural disasters.

To identify the key areas in the provision of information security, we will outline the main types of risks when using an external data center, and ways to minimize them:

− Insufficient level of information security (hereinafter - IS) in the data center. To minimize this risk, one should carefully approach the selection of the data center, and make sure that it meets all the security requirements:
− Receipt of the unauthorized access to customers' information by the data center staff. To avoid this, confidential information must be encrypted. In addition, it is necessary to monitor and record the actions of the staff of the data center. For this, it is necessary to organize additional physical safety circuits for the equipment with remote monitoring and controlling this circuit;
− Lack of access to the data center. Reliable communication channels play a critical role when transferring data or services to an external site. Therefore, one need to make sure that the data center has a reliable data channel reservation;
− The impossibility of direct physical control over the engineering infrastructure of the data center. One need to be able to remotely monitor the critical engineering systems of the data center (power supply and conditioning systems), as well as microclimate parameters;
− Transport accessibility. Territorial remoteness creates additional difficulties with supplementing, repair or replacement of equipment. It is necessary to consider in advance the number of trips to the site and the degree of dependence on them. Also, one must immediately

plan at least two alternative routes, independent of each other, as with the use of public transportation, and without it;

− Data transmission channel. In fact, most remote data centers that are outside the infrastructure of the enterprise itself, must be securely connected and provide "five nines" (this means that 99.999% of the time the service, equipment or facility is operational) and the continuity of the data center access to the rest of the company's infrastructure. Otherwise, the data center generally loses its meaning.

Also, there are a number of other risks, but not less important for minimization:

− short-term loss of manageability of all information resources;
− binding to one data center;
− financial losses in the event of an increase in the cost of services;
− the difficulty of transferring infrastructure to another site;
− probability of long downtime;
− lack of resources for the data center to expand client's infrastructure;
− access by unauthorized persons to the systems, etc.

We should note that today, when considering the topic of data center security, there are many serious security issues for the virtualized environments, the security of storage area networks (SAN), the security of cloud computing and the protection of the connection between the main and backup data centers, etc.

In order to minimize these risks, it is necessary to have a backup site in another data center, where backup copies of the information systems must be kept and constant serious monitoring of the authorized persons must be provided. Also, the organization of disaster-proof solutions that provide synchronous replication of data between data centers will significantly help reducing the risks associated with downtime.

2 Results

Thus, threat modeling or risk analysis that a data center may encounter, has allowed us to define elements for identifying the key areas that should be taken into account when building an information security system:

− network infrastructure;
− the perimeter of the data center;
− network storage;
− server infrastructure;
− virtualization;
− applications;
− connection to the backup data center;
− cloud.

3 Conclusions

Each of the listed elements must undergo a detailed analysis for the study of its weak and strong places. It is necessary to understand that the task of protecting information with a properly built-up security system is mainly to minimize damage at any possible impact, and to predict and prevent such impacts. Also, it is necessary to analyze the whole block of normative legal acts that are directly related to the data center.

In addition, for data centers, it is important to have a developed security policy, strict regulation and developed documentation system, as well as careful planning and compliance with the standards set for the data centers in the TIA-942 standard for telecommunications

infrastructure and other international standards and requirements in this field, and also benefits, directing it to improve the level and quality of life of the population.

References

1. E. Yakovets, *Fundamentals of legal protection of information and intellectual property* (2010)
2. RossiyskayaGazeta, *The Doctrine of Information Security of the Russian Federation: (approved by the President of the Russian Federation on 09.09.2000 №. Pr-1895)* (2000)
3. S. Ozhegov, *Dictionary of the Russian language: 80 000 words and phraseological expressions* (2014)
4. I. Beckman, Informatics http://profbeckman.narod.ru/InformLekc.htm, (2017)
5. On Information, Information Technologies and Information Protection: Federal Law No. 149-FZ of July 27, 2006, Collection of legislation of the Russian Federation, **31 (1 hour)** (2006)
6. V. Turkova, A. Archipova, N. Kitaev, *Improper work of Russian law-enforcement agencies as a determinant of corruption-related crimes committed by government officials* (2017)
7. A. Alexentsev, Questions of Information Protection, **16,** (2006)
8. BS ISO/IEC 27001:2013 (BS 7799-2:2013), *Information technology: security techniques. Information security management systems: requirements* (2013)
9. ISO 9001:2008, *Quality management systems: requirements* (2015)
10. ISO 14001:2004, *Environmental management systems - Requirements with guidance for use* (2015)
11. P. Loncich, E. Kunakov, Problems of Economic Development and Entrepreneurship: Materials of the All-Russian Scientific and Practical Conference, **274** (2016)
12. P. Lontsikh, E. Kunakov, N. Lontsikh, E. Drolova, I. Livshitz, International Conference IT&QM&IS, **754** (2017)
13. A. Bogoviz, S. Lobova, Y. Ragulina, A. Alekseev, V. Garnova, Mediaobrazovanie-Media Education, **3**, 7-14 (2017)