Information security of territorial stability

Anton Nazarov*, *Dmitry* Nazarov, and *Denis* Kovtun

Ural State University of Economics, Yekaterinburg, Russia

Abstract. As a result of the spread of malicious information and spam in the Network, unauthorized access, disclosure, distortion, modification, destruction of both personal data of an individual user and digital data that make up the infrastructure of an entire state are possible. Therefore, ensuring information security is today one of the most important tasks of a society that seeks to preserve the current state of its territory of residence in the conditions of various external influences. Within the framework of information protection, a set of measures is implemented to ensure the security of data while maintaining their availability, confidentiality and integrity. The article deals with the problems of ensuring information security in the context of the transition to the digital economy. The article describes the main challenges and threats to databases in the form of unauthorized use, distortion, modification, and destruction of information. The directions and tools for preserving and protecting information posted on digital resources are defined.

1 Introduction

In modern organizations, information security systems are built on the basis of international standards, taking into account the best international experience. The system of measures includes: detailed instructions and recommendations for users, backup, training of personnel in the basics of information security, installation of security software, regular updates of antivirus programs, data encryption, updating the local network, installation of video cameras, additional servers, uninterruptible power supplies. This significantly reduces the threat of leakage of business information, the adverse impact on the operation of information systems of hacker attacks and fraudulent programs.

An important aspect is the personal information security of users: installing protection against virus programs and regularly updating it, as well as upgrading software, including a web browser; using reliable data storage devices; blocking spam and advertising, potential sources of viruses [1, p.84].

2 Methodology

The goal of creating each user's own information security system is to preserve their data, minimize the risks of unauthorized access to important information, for example, bank cards,

* Corresponding author: nazarovad@usue.ru

accounts, passwords. To do this, you must not use passwords used in other services, carefully check the recipients of payments when registering on mass sites, and use a spare email address.

The transition of developed countries to the digital economy has a positive impact on the efficiency of social production, the level and quality of life of people. However, in the information sphere, there are numerous challenges and threats that cause significant damage to the interests of States and their citizens. Therefore, the activities aimed at ensuring national information security are constantly being improved in order to implement the individual's rights guaranteed by laws to protect against external, internal, artificial and natural information threats [3, p. 71].

External threats to the country's information security include: the use of information technologies by opponents in order to weaken national sovereignty, violate the stability of the economy and public life, as well as the territorial integrity of the state; targeted unauthorized influence of foreign special services on the resources of automated information systems, information and communication networks, automated control systems and telecommunications networks used to ensure the interaction of critical information infrastructure objects; the dominance of individual world powers in the information space due to technical superiority, priority positions in the international competition of information technologies and resources; transnational computer illegal actions (often in the field of finance and credit); disconnection from payment systems, whose services are available in different countries, from air transport AIS.

3 Results and discussions

Internal threats to information security are: the dependence of the country's economy on foreign electronic components of IT; the low level of its own scientific research in the field of IT and their implementation in the production sphere; the disclosure of personal data of users during processing using IT technologies.

Natural disasters, such as hurricanes, earthquakes, tsunamis, and floods, are considered natural threats that are independent of the human will.

Artificial threats include unintentional actions committed by a person due to ignorance or carelessness, as well as deliberate actions in the form of revenge of employees, hacker attacks, encroachments of competitors [4, p. 66].

The core of production in the digital economy is digital data, based on the analysis of which a significant increase in the efficiency of public production is provided: labor productivity increases, equipment downtime periods are reduced, the cost of storing products in warehouses decreases, the speed of launching new products to the market increases and the accuracy of forecasting sales volumes increases.

These processes are negatively affected by:

- violations of the rights of the individual, for example, when correlating the subject with his digital image, ensuring the integrity of the digital data of the citizen;
- the presence of structurally complex information and telecommunications systems of heterogeneous cloud data storage, technological connections, virtualization methods, which pose a danger both for individual individual entrepreneurs and for the entire state;
- powerful external information technology impact on the information infrastructure;
- crimes committed with the use of computers;
- insufficient level of IT development;
- use of network users ' data for commercial and political purposes;

– espionage collection of information about competitors to obtain dishonestly trade secrets.

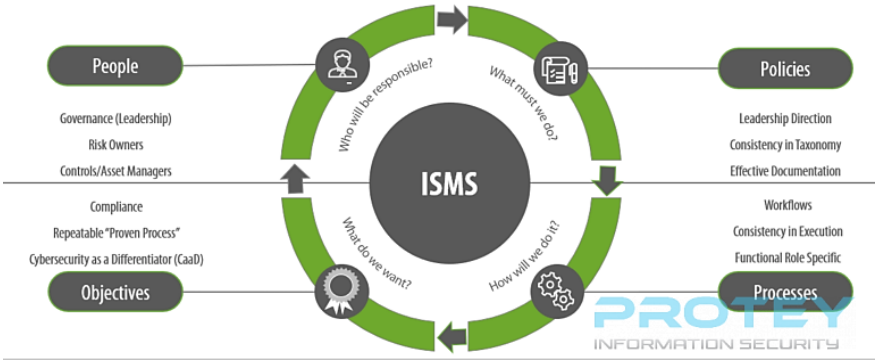

Fig. 1. Information Security Management System (ISMS)

Such a method of data encryption as cryptography has good prospects in the field of information protection, with the help of which it is possible to identify and authenticate objects and subjects of the Internet environment, constantly monitor and differentiate access to arrays of documents in information systems, and ensure guaranteed protection of the totality of data stored in accordance with certain schemes [5, p.136].

Specialists create effective systems of software, information, and analytical tools, through which, with high adaptability and payback, the tasks of preparing the economy, population, and state troops to repel external aggression, protect the independence and territorial integrity of the country, steadily increase the level of well-being of citizens, stable growth of the economic sphere, development of education, science, and culture, and optimal use of natural resources are solved.

These technologies have a number of specific features: a) guarantee the impossibility of falsifying previous data due to their immutability; b) do not require centralized management; c) ensure the storage of information in a simple and reliable form; d) exclude unauthorized access to information by encrypting it; e) allow you to maintain the confidentiality of financial activities; f) prevent the financing of terrorist organizations, laundering of illegally obtained income.

Continuous monitoring in real time, covering all phases of the existence of information from the moment it is received by the user to the moment of its destruction or loss of significance, helps to take into account current threats and vulnerabilities [6, p. 17].

Within the framework of administrative control, compliance with the requirements of regulatory legal documents, compliance with established rules, standards, principles, and procedures is checked.

By means of logical control, the degree of protection of access to information systems, software, passwords, and monitoring data is checked.

Physical control will allow you to assess the state of the workplace environment and computing facilities: air conditioning, fire protection systems, video surveillance, alarm systems, locks.

4 Conclusions

Thus, in order to ensure the information security of the territories ' stability, it is necessary to:

1. Timely and efficiently identify the causes and conditions of unauthorized access to information with the intention of destroying, changing or distorting it.
2. Exclude unauthorized access to data and negative impact on them to prevent information leakage.
3. Regularly identify the vulnerability of information assets through monitoring and in-depth analysis of the information space.
4. Neutralize threats to information security through the integrated use of computer system protection tools.
5. To ensure the unity, stability, and security of the entire information and telecommunications infrastructure of all levels of the territory [2, p. 21].
6. Provide high-quality legal protection of the interests of economic entities and individual citizens in the field of information security.
7. Prevent negative impacts that destroy, distort, destroy information, cause failures in the functioning of information systems.
8. Follow a systematic approach, that is, to ensure an optimal proportion between organizational, programmatic, legal, and physical methods of information protection.
9. Continuously develop the information security system, as each new attack on data is more sophisticated and complex than the previous one.
10. Do not reduce the level of reliability of the system in the conditions of failures, failures, errors, hacks.
11. Actively fight against malicious software, efficiently protect information from viruses.
12. Create physical barriers for intruders to access the information that needs to be protected.
13. Identify users, resources, and personnel of the information security system.
14. Establish the authenticity of users based on their credentials.
15. To allow users to certain working conditions only in accordance with the regulations.
16. Users ' access to resources should be included in special protocols.
17. Respond in a timely manner to unauthorized data access attempts using a system of signals, failures and delays in operation.

References

1. A.I. Akhmetyanova, A.R. Kuznetsova, Basic Research, **8-1**, 82 (2016)
2. A.V. Babkin, D.D. Burkaltseva, D.G. Kosten, Yu.N. Vorobiev, SPbSPU Scientific and Technical Bulletin. Economic sciences, **10(3)**, 9 (2017)
3. D.A. Gorulev, Technical and technological problems of service, **1(43)**, 77 (2018)
4. S.E. Korotchenko, M.E. Listopad, Vestnik NGIEI, **9(64)**, 65 (2016)
5. O. M. Makhalina, V.N. Makhalin, Information Technologies in Management, **1**, 134 (2020)
6. D.V. Udalov, Economic security and quality, **1(30)**, 12 (2018)
7. F. Khochueva, T.L. Shugunov, A.Z. Zhukov, Ch.Kh. Ingushev, Modern high technologies, **11(1)**, 65 (2018)
8. A. Ahmadi, A.E. Nezhad, V. Hredzak, Security-constrained unit commitment in presence of lithium-ion battery storage units using information-gap decision theory. IEEE Transactions on Industrial Informatics, 15(1), 148 (2019).
9. W. Alec Cram, J. D'Arcy, J. G. Proudfoot, MIS Quarterly: Management Information Systems, **43(2)**, 525 (2019).

10. A. Anand, A. K. Singh, Computer Communications, **152**, 72 (2020).
11. D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, Information Processing and Management, **58 (1)**, 102397 (2021).
12. J. D'Arcy, P. B. Lowry, Information Systems Journal, **29(1)**, 43 (2019).
13. A. Ključnikov, L. Mura, D. Sklenár, Entrepreneurship and Sustainability Issues, **6(4)**, 2081 (2019).
14. B. Li, Z. Fei, C. Zhou, Y. Zhang, IEEE Internet of Things Journal, **7(1)**, 33 (2020)
15. N. Miloslavskaya, A. Tolstoy, Cluster Computing, **22(1)**, 103 (2019)
16. D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, Z. Han, IEEE Access, 7, 54508 (2019)
17. J. Wu, M. Dong, K. Ota, J. Li, Z. Guan, IEEE Transactions on Emerging Topics in Computing, 7(4), 553 (2019)