European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.12.02.73

ICHEU 2021
International Conference «Humanity in the Era of Uncertainty»

SOCIO-PHILOSOPHICAL ASPECT OF A SAFE ENVIRONMENT IN THE INFORMATION SPACE

Natalia N. Samokhina (a)*
*Corresponding author

(a) Nizhnevartovsk State University, 56 Lenina Street, Nizhnevartovsk, Russia, natalia58@yandex.ru

Abstract

The modern world is entering a qualitatively new stage in its development, which is manifested in the growth of the technosphere and the renewal of the entire production process through automation and robotization, updating the resource base of production based on informatization, and the comprehensive use of knowledge. The growing role of information and information systems is a historical fact underlying the concepts of the information society. “Information society” is a theoretical concept of a post-industrial society that substantiates a new “historical phase” of the possible development of civilization, in which information and knowledge become the main products of production. The variety of products and services of information activity testifies to the expansion of the social movement of information and knowledge and speaks of the complication of the social configuration and specification of intellectual activities in the conditions of the modern stage of the information revolution. It is important to understand that the effective functioning of the system for ensuring national, state security is impossible without fundamental research aimed at forming an interconnected system of knowledge about the basic principles of the formation and implementation of security threats, as well as about the patterns of organization and content of activities to identify and neutralize them. The authors form a methodological and theoretical basis for conducting applied research and solving practical problems in the field of ensuring the security of the Russian Federation.

Keywords: Information security, information space, Internet, modern society

https://doi.org/10.15405/epsbs.2021.12.02.73
Corresponding Author: Natalia N. Samokhina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The main social function of information security is to ensure the stability and sustainability of the socio-economic and socio-political development of society in accordance with objectively operating laws and trends in the presence of internal and external threats.

In turn, the main social aspect of the content of information security is the system of directions, institutions and features of the functioning of information flows, corresponding or not corresponding to the nature of the performance of the subjects of management of their social functions.

It should be noted that the level of protection of personal data is insufficient, which in practice leads to various negative consequences.

2. Problem Statement

Ensuring information security is one of the key tasks of society. It was important in the past and during the pandemic it acquired special significance, as the number of cybercrimes increased.

3. Research Questions

The subject of the research is the state and methods of ensuring information security in modern conditions.

4. Purpose of the Study

The purpose of the study is to identify and eliminate sources of threats to information, to determine the causes and conditions that contribute to damage, as well as to find ways to eliminate them and describe these methods.

5. Research Methods

The methodological base consists of methods of complex and systemic analysis based on interdisciplinary research of topical problems (basic concepts, subject matter, structure of information and security, as well as relations arising in connection with this and their reflection in the law and legislation of Russia); general scientific methods of cognition.

6. Findings

When studying the social aspects of information security, important indicators are:

- the degree of awareness of various social strata and groups of the population;
- social feelings, moods, stereotypes;
- attitudes in the field of law abiding and use of information;
- legitimate interests.

An integral indicator of the information security of modern society is social activity in the information space.

https://doi.org/10.15405/epsbs.2021.12.02.73
Corresponding Author: Natalia N. Samokhina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Numerous studies are mainly focused on the study of individual situations of interaction with the Internet space, its psychological influence on a person, on the danger / safety of this influence, as well as on the methodological features of teaching using information and communication technologies.

Firstly, various types of activity (first of all, learning) do not occur exclusively in the digital environment, “live” interaction is still preserved; therefore, it is pertinent to pose the question of what is the sphere of activity, where two environments are combined: digital and pre-digital?

Do we have the right to say that this environment is fundamentally new, indefinite, having its own conceptual load?

Secondly, the global scale and variety of digital resources of the modern information environment create not only new opportunities, but certain risks, the understanding of which is important for the safety of the subject of communicative interactions in the system of relations "individual - information (digital) environment".

Thirdly, this raises the question of what are the perceptions of various communities about the risks of the Internet; How does the subject grow into the digital environment?

Fourthly, to what extent the eco-psychological approach to the development of the psyche and the subject of environmental interactions allows analyzing the transition and merging of the pre-digital and digital information environment, as well as conceptualizing the communicative interactions of the system of relations "individual - information (digital) environment".

The life of a modern person, his life activity, education, personal and professional development is already unthinkable to imagine outside of communicative interactions with the information environment, and now they increasingly speak - a digital environment, for which they use terms such as: information space, cyberspace, Internet environment, media space.

To do this, it is necessary to turn to the terminology.

> Streltsov and Pilyugin (2019) says: information society is a society in which information and the level of its use and accessibility radically affect the economic and socio-cultural living conditions of citizens. Information space is a set of information resources created by subjects of the information sphere, means of interaction of such subjects, their information systems and the necessary information infrastructure. (p. 26)

Digitalization of the information environment involves communicative interactions in the system of relations "individual - information (digital) environment". Therefore, this monograph is devoted to the application of an ecopsychological approach to the development of the psyche, built on the relationship "individual - environment", to analyze what the digitalization of the information environment of a modern person is at the stage of its transformation into a digital environment and what psychological risks arise in this case (Peltier, 2016).

One of the main points of security is to provide each employee of the enterprise with the minimum level of privileges of access to the database and information system that they need to perform their job duties. Provided that the majority of security breaches originate from their own employees, the introduction of clear restrictions is very important.

https://doi.org/10.15405/epsbs.2021.12.02.73
Corresponding Author: Natalia N. Samokhina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Cryptography opens up solutions to many network information security problems: authentication, confidentiality, integrity, and control of interacting participants. The term "Encryption" means the transformation of data into a form that is not readable for humans and software systems without an encryption-decryption key. Cryptographic methods of information security provide information security means, therefore it is part of the information security concept. The most important component of the cryptographic method of protecting information is the key, which is responsible for the choice of transformation and the order of its execution.

A key is a certain sequence of characters that sets up the encryption and decryption algorithm of the cryptographic information protection system. Each such transformation is uniquely determined by a key that defines a cryptographic algorithm that ensures the protection of information and information security of the information system (Blinov, 2020).

One of the foundations of information security in cryptography is data integrity.

Information protection in local networks and information protection technologies along with confidentiality are obliged to ensure the integrity of information storage. That is, the protection of information in local networks must transfer data in such a way that the data remains unchanged during transmission and storage (Andress, 2014).

In order for information security of information to ensure the integrity of data storage and transmission, it is necessary to develop tools that detect any distortions of the original data, for which redundancy is added to the original information. Information security in Russia with cryptography solves the issue of integrity by adding a certain checksum or check combination to calculate the integrity of the data (Prikhodko, 2019).

According to representatives of the IT sphere, the vulnerability of SMEs was mainly due to:

the need for prompt decision-making. We are accustomed to the fact that we have been implementing information security projects for months, quarters and years, but in the current conditions, in fact, it was necessary to make decisions within a few days or weeks, provide employees with equipment and revise approaches to work organization;

blurring the boundaries between corporate and personal devices, corporate and personal data - this is due to the fact that many employees work from home on their personal laptops and computers, which a priori have a lower level of protection than corporate resources;

the dependence of information security on people and the insufficient level of knowledge of employees about threats to information security, about methods of their recognition based on their primary characteristics and ways of countering them;

insufficient funding for information security or even a reduction in the cost of this;

problems with import substitution, in particular, a shift in the timing of replacing imported hardware, etc. (Malyuk, 2016).

Meanwhile, experts believe that during the period of the spread of the new coronavirus infection, the role of information security has significantly increased in general.

In this regard, experts identified the following among the key recommendations for business:

the need to develop protective solutions, network policy in the company;

use, whenever possible, the services of professional outsourcing companies;

https://doi.org/10.15405/epsbs.2021.12.02.73
Corresponding Author: Natalia N. Samokhina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

use of information security protection mechanisms operating in automatic mode;

education of employees, familiarizing them with information security measures through seminars, trainings on the topic;

sufficient funding for the task of ensuring information security, since a reliable data protection system will not only prevent direct theft of databases and other corporate information, but also, in general, ensure the smooth operation of the organization and improve business efficiency (Zegzhda & Ivashko, 2020).

Considering the issue of ensuring information security in companies, it will be important to recall the Letter of the Federal Service for Technical and Export Control of March 20, 2020 No. 240/84/389, which contains a list of recommendations for ensuring security during the implementation of remote operation in terms of critical facilities, information infrastructure. The document is addressed to government agencies, government agencies, Russian legal entities and individual entrepreneurs who legally own information systems, information and telecommunication networks, automated control systems operating in the fields of health care, science, transport, communications, energy, banking, etc., but will useful to other subjects.

In addition to instructing employees working remotely on the rules for secure remote interaction and the undesirability of using personal computer equipment (hereinafter referred to as SVT) for remote access, FSTEC advises:

determining the list of information and information resources (programs, volumes, directories, files) located on servers to which remote access is provided;

providing the minimum necessary rights and privileges to users when working remotely;

identifying remote SVTs by physical addresses on servers to which remote access will be provided;

excluding the possibility of operation of remote SVT by unauthorized persons;

organizing secure access from a remote SVT to servers using cryptographic information protection tools (VPN client);

using anti-virus information protection tools on remote SVTs, ensure the relevance of the databases of signs of malicious computer programs (viruses) by updating them daily;

excluding the possibility of an employee installing software on a remote SVT, except for software, the installation and operation of which is determined by service necessity;

ensuring monitoring of the security of information infrastructure facilities, including by keeping logs of actions taken by employees of remote SVTs and analyzing them;

blocking the user's remote access session if the user is inactive for more than a specified time;

ensuring the ability to respond quickly and take measures to protect information in the event of computer incidents (Zharova, 2020).

The above measures will minimize the risks of additional threats to information security when employees remotely access corporate systems during the period of the threat of the spread of a new coronavirus infection (Samokhina, 2021).

Taking into account the basic rules of "digital hygiene", experts advise one to:

- not open suspicious files;
- use different passwords to access services, that is, not a single username and password for all sites;

- compose complex passwords and change them periodically;
- not write down passwords and not store them all in one file, or use a password manager for this, which provides additional data protection;
- use trusted sources of information.

7. Conclusion

The topic of ensuring information security and combating cybercrime, which in recent years has been among the key global risks, is gaining momentum during the spread of the new coronavirus infection. And if earlier representatives of the industry focused on combating attacks by malefactors, now the priority is given to protecting information and preventing possible threats. Therefore, experts urge users to rethink the approach to information security and minimize the "attack area" as much as possible, and use the useful lessons on information security that they received during the pandemic during the post-pandemic period.

We note that the problem of information security is included in the priority list. So, within the framework of the federal project "Information Security" of the national program "Digital Economy of the Russian Federation" (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, minutes of December 24, 2018 No. 16) (Passport of the national program, 2018), by the end of 2021 year, it is planned to develop and adopt a set of information security standards, ensuring the minimization of risks and threats to the safe operation of public communication networks.

References

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice.* Syngress.

Blinov, A. (2020). *Information Security.* Textbook. Publishing house of SPbGUEF.

Malyuk, A. (2016). Foreign experience of forming a culture of information security in society. *Security of information technologies, 4.*

Passport of the national program. (2018). "Digital Economy of the Russian Federation" (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, minutes of December 24, 2018 N 16).

Peltier, T. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management.* CRC Press.

Prikhodko, A. (2019). *Information security in events and facts*. SINTEG.

Samokhina, N. (2021). Information Culture in the Context of Remote Interaction. *Proceedings of the VIII International Scientific and Practical Conference 'Current problems of social and labour relations' (ISPC-CPSLR 2020)* (pp. 589–593). Atlantis Press. https://doi.org/10.2991/assehr.k.210322.181

Streltsov, A. A., & Pilyugin, P. L. (2019). On the issue of digital sovereignty. *Informatization and communication, 2.*

Zegzhda, D. P., & Ivashko, A. M. (2020). *Fundamentals of information systems security.* Hotline-Telecom.

Zharova, A. K. (2020). Legal classification of threats and risks in the information sphere. *Questions of defense technology. Series 16: Technical means of countering terrorism, 7-8,* 97-98.