European Journal of Emerging Technology and Discoveries
ISSN (E): 2938-3617
Volume 2, Issue 10, October - 2024

GENESIS, NATURE, CONCEPT AND STRUCTURE OF CYBERSECURITY IN PHILOSOPHICAL DISCOURSE

Sobirov Anvar
Scientific Researcher
E-mail: dilm79@inbox.ru Mobile +998997700429

Abstract
The intensive development of information technologies over the past 50 years has greatly changed the world in all spheres of public life. Global informatization of society is one of the dominant trends in the development of human civilization in the 21st century. "The rapid development of information technologies, the increase in the capabilities of telecommunication systems leads to the emergence of new challenges and threats committed in cyberspace." Currently, we can note a significant average annual increase in the number of incidents in the field of information security, affecting a wide range of private corporate, as well as state interests. The current situation suggests an increase in the importance of cybersecurity in the information security system.

Keywords: cybersecurity, cyberspace, cyber threat, cyber danger, information security, information space, cyber threat, information danger.

Introduction

Currently, we can note a significant average annual increase in the number of incidents in the field of information security, affecting a wide range of private corporate, as well as state interests. The current situation suggests an increase in the importance of cybersecurity in the information security system. The main terms related to the field of cybersecurity, such as "cybersecurity", "cyberspace", "cyber threat", and "cyber danger" are in many ways similar to the terms "information security", "information space", "information threat", "information danger". Thus, to define the concepts of cybersecurity, first of all, it is necessary to consider the terms related to information security to separate the former from the latter.

Thus, to define the concepts of cybersecurity, first, it is necessary to consider the terms related to information security to separate the former from the latter.

The concept of "information space" in the Russian scientific community was first used by O.V. Kedrovsky in his work "Information Space of Russia" (Kedrovsky. 1994). Subsequently, it was considered in the works of S.A. Modestov, I.M. Dzyaloshinsky, A.S. Chuprov, N.B. Zinovieva, E.M. Palena, and S.E. Zuev. First of all, to define the concept of "information space" it is necessary to consider the fundamental terms "information" and "space". In the Federal Law of the Russian Federation No. 149 "On Information, Information Technologies and the Protection of Information" dated April 3, 2005, information means data (messages, data) regardless of the form of their presentation" (Federal Law. 2005). In the Philosophical Dictionary edited by I.T. Frolov The term "space" means "a concept that characterizes the mutual arrangement of coexisting objects" (Philosophical Dictionary. 2001). Therefore, by combining the two concepts, "information space" can be defined as the interaction of subjects and objects of the environment, connected by the processes of production and consumption of information.

In I.M. Dzyaloshinsky's work "Information Space of Russia: structure, features of Functioning, prospects of evolution," an analysis of the main approaches to the definition of the concept "information space" was carried out, highlighting the "geopolitical", "social", and "noosphere-information" approaches (Dzyaloshinsky, 2001).

From the point of view of the geopolitical and philosophical approach, information space is understood as a certain virtual territory belonging to the state, which is a kind of state resource and must be protected from external encroachments. Subject territory. A distinctive feature of this type of information space is the presence of borders. Within this space, there are information resources, information sources, various technical devices that process information, and users of information resources, which in turn fall under the jurisdiction of the legislation in force in the territory of a given state.

Literature Analysis

According to the social approach, the information space is a sphere of relations between people to exchange information. The information space is considered a community of certain structures interacting based on information relations. "For example, in the work of Likhtin A.A. and Kovalev A.A., the information space is defined as an integral part of the social space, in particular its political component" (Likhtin. 2017).

The noospheric-informational one defines the information space as a certain set of information resources belonging to no one, means of ensuring their replenishment and processing, as well as mechanisms for user access to these resources.

In modern Russian science, the definition of current information security issues has become the subject of comprehensive studies conducted by I.A. Lazarev (Lazarev. 2005), V.N. Lopatin (Lopatin. 2007), Yu.S. Ufimtsev and E.A. Erofeev (Erofeev. 2003).

In the work of A.A. Chebotareva, the main scientific approaches to defining the concept of "information security" are considered. "The philosophical approach is based on the identification of three components: satisfying the information needs of subjects; ensuring information security; ensuring the protection of subjects" (Chebotareva. 2011). "Information security is a state of an object in which the state of the information environment allows maintaining the ability and possibility to make and implement decisions by the objectives of the object" (Atamanov. 2007). "The technical approach is focused primarily on the problem of developing security standards, including server protection, licensing, certification and attestation of information technology objects, the use of cryptographic systems when transmitting data via communication channels and other information security mechanisms" (Protsenko. 2008).

In sociology, information security is considered within the framework of the sociology of informatics - one of the areas of sociology.

In jurisprudence, there is also no unified approach to defining the concept of "information security". Lopatin V.N. gives a definition of "information security as a state of protection of the vital interests of an individual, society and the state from negative information impact" (Lopatin.2000). Streltsov A.A. believes that "ensuring information security is a complex process that includes a security object consisting of a set of information needs of the state,

activities to meet these needs, threats to the security object, and the process of counteracting threats." (Streltsov. 2011).

Discussion

Such differences, "in terminological usage and legal meaning, are largely due to the relevance of their translation into the national language." Nevertheless, in domestic and foreign literature, as well as in regulatory legal acts of different countries, terms containing the prefix "cyber" are increasingly encountered, the meaning of which is hidden behind the term "cybernetics" - (from the Greek "art of management") - the science of general patterns of control processes and information transfer in machines, living organisms and society" (Ozhegov. 1997).

There have been active discussions around cyberspace for a significant period, but there is no unambiguous interpretation of this concept. An unambiguous interpretation of the term cyberspace is impossible for three reasons. The first is the identification of cyberspace and the Internet space. The second is the substitution of the concepts of cyberspace and virtual reality. The third is the high speed of development, implementation and dissemination of new technologies create serious obstacles to the implementation of relevant analysis. Wellman B. in his work ""Physical place and Cyberplace: the rise of Personalized Networking" considers cyberspace as a tool for organizing the real world, which also becomes a place for people to live and coexist alongside physical space, which continues to retain its importance" (Wellman.2001).

From the point of view of the physical or material perception of cyberspace, the presence of certain devices by means of which cyberspace is created and functions is important. Cyberspace is a virtual place created by a network of interconnected computers in which agents interact.

To understand the content of the terms cyberthreat and cyberhazard, it is advisable to turn to the concepts of "danger" and "threat". Danger is an objectively existing possibility of a negative impact on a certain object, as a result of which it may be damaged, or harmed, worsening its condition, and giving its development a negative dynamic. The threat is a danger at the stage of readiness to move from possibility to reality." Therefore, in the broadest sense, the term "cyber threat" can be defined as a set of conditions and factors characterized by a real possibility of violating cyber security by illegal malicious penetration into virtual space to achieve political, social or other goals. The term "cyber danger" accordingly, is a set of conditions and factors that, under certain conditions, can lead to the emergence of a cyber threat. It is worth noting that the international community has not yet come to a common understanding of key terms in the field of cyber security. Two main approaches to defining cyber security can be distinguished: a broad approach and a narrow approach. Within the broad approach, the concept of cyber security includes both technical and psychological aspects. The narrow approach is limited exclusively to technical aspects. For example, "in the cyber security strategy of Sweden, cyber security is understood as a set of security measures aimed at maintaining the confidentiality, reliability and availability of information." In turn, "Germany uses a narrow approach in its cybersecurity strategy, where cybersecurity is defined as a desired goal of information security, a situation in which the risks of German cyberspace have been reduced to an acceptable minimum." In some scientific works, "cyber threats and cyber hazards are considered as a set of threats and dangers to information security. G. Kerschischnig, in his

study" (Kerschischnig. 2012), devoted to the problem of cyber threats, uses a number of terms denoting different degrees of danger to information security. In particular, he provides the following terms: "cyber interference" is the most general concept; "cyber incident" - incidents in cyberspace that have remained unpunished; "cyber attack" - any attempt at destructive impact on a device; cyber war - confrontation and confrontation in cyberspace." The set of listed terms, in this case, will be designated as "cyber threats".

In the international standard ISO 27032, which is implemented in the style of a risk-oriented approach and which defines cyberspace assets and stakeholders, threats, recommendations and risk treatment measures, cyberspace is formulated as a complex virtual environment formed as a result of the actions of people, programs and services on the Internet through the appropriate network and communication technologies. By analogy with the classical definition of information security, the standard understands cybersecurity as the property of asset protection from threats to confidentiality, integrity, and availability in cyberspace. The standard does not provide a definition of cyber threats, however, based on the diagram "Basic concepts of cybersecurity and the relationship between them" given in the standard, it can be concluded that a cyber threat is the use of vulnerabilities of an information system by cyber threat agents for the illegal use or damage of information system assets. The document also contains the concept of "Risk" of cybersecurity, which can be defined as the degree of probability of cyber threats. Cybersecurity is the protection of systems (hardware, software and data) connected to the Internet from cyber threats. The concept of cybersecurity is very multifaceted and therefore difficult and hard to formalize. There are many different ideas and views here.

Information security specialists and simply interested users, in particular, those who left comments on the Concept, express very contradictory views on this issue. Analysis of comments shows that one of the main problems in the development of such documents is the difficulty of understanding the term cyberspace and the related concept of cybersecurity.

"Cyberspace is a sphere of activity in the information space formed by a set of communication channels of the Internet and other telecommunication networks, the technological infrastructure that ensures their functioning, and any forms of human activity (individuals, organizations, states) carried out through their use."

Conclusion

In principle, such a definition to some extent interprets individual aspects of this important concept, but the lack of further detailed explanations leads to an inaccurate understanding of it. The vast majority of experts who left their comments on the draft Concept believe that the definition deals exclusively with the technological component of the information field, that is, with the computer and telecommunications infrastructure. The issue of activities based on this infrastructure and any types of human activity carried out through technology is completely omitted from consideration. And this is directly stated in the definition. For a document of such great importance, this is unacceptable and indicates the need for further methodological work on defining cybersecurity as a characteristic of cyberspace. Cyberspace is a complex environment that does not exist in any physical form, arising as a result of the interaction of people, software, and Internet services through technological devices and network connections. "In a program article on cybersecurity, UK experts define this concept as any activity in a

network, digital form, adding after that that this also includes information content and actions carried out through digital networks." (Klimburg A. et al. 2012)

From a philosophical point of view, the concepts of "cybersecurity" and "information security" are often used as synonyms. However, in reality, these terms are very different and are not interchangeable. Cybersecurity is understood as protection against attacks in cyberspace, and information security is the protection of data from any form of threats, regardless of whether they are analogue or digital in the information society.

Cybersecurity practices can be applied in a variety of areas - from industrial enterprises to mobile devices of ordinary users:

Critical infrastructure security - measures to protect computer systems, and networks of critical information infrastructure (CII) facilities. CII facilities include electrical networks, transport networks, automated control systems information and communication systems and many other systems, the protection of which is vital for the security of the country and the well-being of citizens.

Network security - protection of the basic network infrastructure from unauthorized access and misuse, as well as from theft of information. The technology includes the creation of a secure infrastructure for devices, applications and users.

Application security is security measures applied at the application layer to prevent theft or compromise of application data or code. Methods cover security issues that arise during the development, design, deployment, and operation of applications.

Cloud security is an interconnected set of policies, controls, and tools that protect cloud computing systems from cyber threats. Cloud security measures are aimed at ensuring the safety of data, online infrastructure, and applications and platforms. Cloud security has some common concepts with traditional cybersecurity, but it also has its own best practices and unique technologies.

Types of Cybersecurity Threats

Cybersecurity technologies and best practices protect critical systems and sensitive information from the rapidly growing volume of sophisticated cyberattacks. The following are the main types of threats that modern cybersecurity combats:

Malware

Any program or file that can cause damage to a computer, network, or server. Malware includes computer viruses, worms, Trojans, ransomware, and spyware. Malware steals, encrypts, and deletes sensitive data, modifies or hijacks core computing functions, and monitors the activity of computers or applications.

Social Engineering

A method of attack that relies on human interaction. Attackers gain the trust of users and force them to violate security procedures and give up sensitive information.

Cryptojacking

A relatively new type of cybercrime in which malware hides in the system and steals the computing resources of the device so that the attackers can use them to mine cryptocurrency. The process of cryptojacking is completely hidden from the eyes of the users. Most victims become suspicious when they notice an increase in their electricity bills.

References

1. Kedrovsky O.V. Information space of Russia / O.V. Kedrovsky // Information resources of Russia. -1994. - No. 4. - P. 2-3.
2. Philosophical dictionary / Ed. I.T. Frolov. — M.: Respublika, 2001. — P. 356
3. Dzyaloshinsky, I. M. Information space of Russia: structure, features of functioning, prospects of evolution / I. M. Dzyaloshinsky. - Mosk. Carnegie Center, M.: - 2001. - 30 p
4. Likhtin, A. A. Theoretical aspects of the concept of "information policy" and features of its implementation in modern Russian socio-political reality / A. A. Likhtin, A. A. Kovalev // Management consulting. - 2017. - No. 1 (97). - P. 32
5. Lazarev, I. A. Information and security. Composition technology. M.: Publishing house of the Moscow city centre of scientific and technical information, 2002.
6. Lopatin, V. N. Information security of Russia: man, society, state / V. N. Lopatin // Series: Security of man and society. SPb.: Fund University, 2000. P. 428.
7. Ufimtsev Yu.S., Erofeev E.A. et al. Information security of Russia. Moscow: Exam, 2003.
8. Chebotareva A.A., Scientific approaches to defining the concept of "information security" / A.A. Chebotareva // Information law - 2011. - No. 1. P. 3-6.
9. Atamanov G.A. Information security: essence and content / G.A. Atamanov // Business and security in Russia. - 2007. - N 47. - P. 108.
10. Protsenko E.A. Model and method for analyzing the effectiveness of information security systems for websites of government bodies of the Russian Federation: Abstract of Cand. Sci. (Technical) Dissertation / E.A. Protsenko - SPb., 2008.
11. Lopatin V.N. Information security of Russia: man, society, state / V.N. Lopatin // Series: Security of man and society. SPb.: University Foundation, 2000. - P. 428.
12. Streltsov A.A. The content of the concept "ensuring information security" // Information society. - 2001. - No. 4. - P. 16.
13. Ozhegov S.I., Shvedova N.Yu. Explanatory dictionary of the Russian language: 80,000 words and phraseological expressions. - 4th ed., Moscow, 1997. - 944 p.
14. See Wellman B. Physical place and cyberplace: the rise of personalized networking // International Journal of Urban and Regional Research. 2001. Vol. 25 (2). P. 247.
15. Kerschischnig G. Cyberthreats and International Law. / G. Kerschischnig - The Hague, 2012. - P. 5.
16. Markov A.S. Cybersecurity Guidelines in the Context of ISO 27032 / A.S. Markov, V.L. Tsirlov // Cybersecurity Issues. 2014. No. 1 (2). URL: https://cyberleninka.ru/article/n/rukovodyaschie-ukazaniya-po-kiberbezopasnosti-v-kontekste-iso-27032 (accessed: 23.05.2020).

ISSN (E): 2938-3617
Volume 2, Issue 10, October - 2024

17. Federal Law of April 3, 2005 N 149 "On information, information technologies and information protection" [Electronic resource] // Access mode: http://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (date accessed: 04/17/202020).
18. Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). - 2012. http://belfercenter.hks.arvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf.