
Essence and Conceptual Foundations of The Concept of Information Security

Mamadjanov Alisher Muratovich*

Methodological Training Cycle of the Faculty of Military Education, Uzbekistan

DOI:

<https://doi.org/10.47134/academia.v1i2.11>

*Correspondence: Mamadjanov Alisher Muratovich

Email: mamadjonov_a@gmail.com

Received: 04-06-2023

Accepted: 06-06-2023

Published: 15-06-2023

Abstract: This article examines the essence and conceptual foundations of the concept of information security. The influence of information threats and attacks on the development and formation of youth.

Keywords: Information Systems, Telecommunication Technologies, Informatization, Information Threats, Information Security, Information Resources



Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Introduction

Information systems and telecommunication technologies have started their rapid development in the XXI century. They have penetrated almost all spheres of human life and activity (Y. Zhang, 2022).

There is a need for people to actively exchange information within the country and in the outside world. And this may become a factor determining the development of human potential in the XXI century (Khando et al., 2021).

Uzbekistan has developed a State policy on the informatization of society, the development of information resources is based on a legal framework, and the National Information System is being implemented on the basis of world principles (Brazevich et al., 2020).

Methodology

Uzbekistan identifies as a separate area the issues of ensuring information security and improving the information protection system, timely counteraction to threats in the information sphere, prevention of information attacks, and fostering a culture of access to information resources among the youth. [1.-B.39]

Today, planning and management of information production and improving the quality of economic development are becoming increasingly important for all spheres of our social life in general. This is, of course, the positive side of information, but there is also a negative side, that is, the harmful side, which is not only considered threatening to the life and future of man, but also destroys the life of society (Smallwood, 2019).

Taking these two sides of the issue into consideration, information can be categorized into the following types (Cristea, 2020):

1. Socially useful information.
2. Malicious information.

Socially (socially) useful information is information aimed at development, enrichment and increase of labor productivity, ensuring peace and happiness of society and people.

Malicious information is information aimed at undermining, destroying the life of society and people, undermining peace (Tanwar et al., 2020).

Currently, the concepts of "information threat", "information attack" are widely used in scientific consumption. If we pay attention to the etymology of these concepts, we can conclude that they can be used as synonyms.

Information attack or threat is a set of conditions and factors that create a threat to the vital interests of an individual, society and the state in the field of information.

In general, natural and technical sciences, security and its forms have an independent direction by nature. The security aspects of politics, economics, ecology, information, military, etc. are often developed by general sciences. In the formation of a general theory, each of them makes its own contribution. The objective conditions for the creation of a general theory are the following:

1. Making a demand by an individual, organization, social group, society, state and world community for self-preservation and development from the point of view of security;
2. Creation of a security system to protect important objects of life activity of an individual and humanity as a whole from threats;
3. Relates to the creation of a modernized security system capable of resisting massive negative impacts.

A person may be considered as a subject of security, while nature, technical means, real estate, legal and legitimate interests of citizens, society, and the state may be considered as an object. One and the same person himself can be both an object and a subject.

The concept of "security" has a subjective meaning according to the ordinary human imagination, that is, security is the state of a subject protected from negative factors that harm him. In other words, it can be described as "protection", "absence of danger". [2.-B.67] S.I.Ozhegov also gives the following comments on the concepts of danger and threat: in turn, the antonym of "safety" is "danger, threat, harm". [3.-B.38] The concept of "threat" is a possible danger, intimidation, evil to someone, causing harm. [3.-B.39] Thus, the concept of "safety" can be interpreted as the absence of danger for someone, for something (Wulf et al., 2019).

Result

Today there are different definitions of security, the authors of which proceed from different criteria. Sometimes 'security' is status, development traditions and living conditions..." [4.-B.13], as they imagine. as they envision it. In addition, if security limits the development of innovation, it can lead to the factor of stagnation, conservatism, regression. In modern encyclopedic dictionaries this word is interpreted in one way or another. But, we have not encountered the interpretation of prevention, which has an important property and function of security - to reduce, eliminate danger and threat, comprehensively disclosed in the literature. In particular, the meaning of "protection" reflects an important function of security, but it does not mean complete. Much of the literature describes "safety" as "the absence of risk that can cause harm." These definitions, which can be taken at face value, embody two principles of safety (Herath et al., 2020).

The security principle from the second definition, based on the assumption that "complete" security cannot be ensured, relies on the always-existing assumption that a situation of harm occurs. Thus, different cultures around the world have developed, as a rule, the same conceptions of security and threat, emphasizing the individual's anticipation and concern about his or her current and future state. That is, security for a person is first of all his knowledge and perception that he is protected from dangerous actions of various manifestations (Veiga, 2022).

In order to protect the important objects of the country and its citizens, society and the state from external and internal threats, a security system will be established in each state, which will include the composition of security objects and security actors as a key element. According to etymology, the word "security" means that there is no danger. Based on this, it will be necessary to investigate the concept of "danger" or "threat", which is its opposite, in order to substantiate the meaning of the concept of "security". The emergence of the

concept of “danger” is associated with negative factors, that is, as a result of it, the right of people to preserve their lives and health is violated, and in the case of organizations and production enterprises - existence and development, the organization and production enterprise can completely stop. Thus, the formation of the concepts of “safety” and “risk” is directly related to “unplanned” losses in the process of everyday life and activities of people and organizations (Meulemeester et al., 2020).

The security of most objects (entities) is an important structural component in all spheres of society, and its subject (or product) is information. The presence of risk in relation to these objects or entities is the basis for thinking about information security. It is known that all forms of risk are associated with the corresponding information processes. Thus, information security describes the information field, which together forms social relations and is directly related to information and information infrastructures as objects of the individual, society and the state. [5.-B.39] The problem of national security also has a clearly defined information description. [6.-B.3] These circumstances together with the task of building a strong civil society make information security a priority issue of ensuring national security as a result of the growing importance of information, the development of information resources and technologies in the state (Toth, 2022).

It is known that national security is realized in two forms: at the public and state level, which in turn are divided into internal and external depending on the source of danger. Personal security has the first level and determines the security of the state and civil society.

Persuasive information is a conscious action of the subject of information (source), which can act on the basis of a clearly defined goal, assuming the obligation to exert its influence on a particular social object (a person, social group, public institution, etc.).

Encouraging information can be positive or negative, for example, if the inducing information is negative, its activity can conflict with the interests of the object and derail it. These actions are either explicit or implicit and affect the subject's psyche.

Based on the above considerations, we can come to the following conclusion: security is the ability of a system to fight threats, as well as the ability to achieve a high level of its development.

So, security is a description of the existence of any object, the ability of this object to protect its values, goals, interests, in other words, the basis for the existence of the system, to fight against threatening forces.

Information security is a unique phenomenon of modern society, which is of global importance for all mankind and is characterized by the fact that the formation of its objective, practical definition is a vital necessity (H. Zhang et al., 2019).

According to experts, the difficulty of explaining the problem of information security is due to the fact that there is still no explanation of this concept accepted by the general

public, it is explained in relation to the field of science. That is why it is necessary to clarify that “security” does not exist without an object. As rightly noted by A.A.Streltsov, “without a concrete object, the concept of ‘security’ acquires an abstract character, it loses its inner essence”. [7.-B.12]

Discussion

We can also name several reasons explaining why it is difficult to interpret this concept as information security as a complex phenomenon:

1. information security is an objective phenomenon associated with the objective conditions of society development. Its formation occurs in connection with the process of informing society.
2. Difficulties in defining the concept of “information security”, in our opinion, are related to its study in connection with various - technical, legal, psychological, pedagogical, social aspects. Of course, scientists define this concept in different ways depending on the sphere of their scientific activity. This creates a number of difficulties in forming a single definition of the term “information security” (Pham et al., 2019).

It has become a tradition in sociological and psychological literature to use the term “information psychological security”. Information-psychological security is an important activity aimed at protecting the state, society and the individual from accidental or deliberate information impact.

Ensuring information security in the modern globalized space serves to prevent damage to the information sector. In this process, it is natural to prevent damage, which can be caused at different levels, as well as to fight against the interference of intruders (Anand & Singh, 2020).

M. Kuronov in his book “The Truth We Understand” in the rubric “Attention, Internet” expressed the following thoughts: “It seems to be too early to make a definite conclusion about the role of the Internet in human life. “Technology is a business. Connect magazine had some troubling words in an article titled “Information + Nation” in its 10th issue of 2003. “In independent Internet users,” the magazine wrote, “stable self-identity, originality, is disappearing. A person's self-perception becomes blurred or unstable...” [8.-B.5-6] U. Gafurov states that the culture of information consumption in the most general sense means a system of knowledge, skills and abilities that serve to obtain, sort, understand and interpret information that serves human interests, maturity and development of society. [3.-B.285] According to B. Khodjaev, the concept of “information consumption culture” reflects three main levels of information security of a person: general, professional and content-value. These levels of information consumption culture development in a person are associated with the choice of specific criteria and indicators of personal development.

Cognitive-operational and organizational components in the system of information consumption culture are determined by the universality, interdisciplinary connection of information activity, as well as computer literacy, which reflects a generalized description of a person in various activity systems. [10.-B.120]

Ensuring information security requires, first of all, studying the negative consequences arising from the use of information technologies, preparing people to protect themselves and members of society from these negative consequences, and preventing emerging problems (P. Zhang et al., 2019).

The threat of harmful (malicious) information is the danger of negative impact on human spirituality and consciousness through messages and information (Veiga et al., 2020).

Conclusion

The following opinion can also be expressed about the occurrence of risks: The occurrence of risks can be different depending on certain conditions. In this regard, some authors use the concept of threat as a concept that reflects the probability of occurrence and concretizes a certain risk, despite the fact that its realization is a logically complex issue. [11.-B.122]

According to the above definitions, the concept of information threat can be defined as follows: it is a set of conditions and factors that threaten the vital interests of an individual, society and the state in the information sphere.

References

- Anand, A., & Singh, A. K. (2020). An improved DWT-SVD domain watermarking for medical information security. *Computer Communications*.
<https://www.sciencedirect.com/science/article/pii/S0140366419317992>
- Brazevich, D. S., Safronova, Z. S., Kosheleva, T. N., & ... (2020). Analysis of the Problems of Ensuring Information Security in the Terms of the Contemporary Society. *Open Journal of Social ...*.
<https://www.scirp.org/journal/paperinformation?paperid=98599>
- Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information ...*.
<https://www.ceeol.com/search/article-detail?id=879221>
- Dahl, V. I. (2002). *Explanatory dictionary of the Great Russian language*. Moscow: [Publisher].

- Decree of the President of the Republic of Uzbekistan. (2017). On the strategy of actions for further development of the Republic of Uzbekistan. Collection of legislative acts of the Republic of Uzbekistan.
- Gafurov, U. (2013). Actual issues of effective use of the Internet in the protection of young people from ideological threats in the face of religion in the conditions of globalization. In Army - state support, guarantee of peace: Methodical manual for the bodies of educational work in the system of the Armed Forces, as well as for propagandists (pp. [page numbers if available]). Tashkent: Sano-Standart.
- Grachev, G. V. (2000). Information-psychological safety of a personality: Theory and technology of psychological protection (Doctoral dissertation). Moscow: [Publisher].
- Herath, T. C., Herath, H. S. B., & D'Arcy, J. (2020). Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. ... for Advances in Information Systems. <https://doi.org/10.1145/3400043.3400046>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security. <https://www.sciencedirect.com/science/article/pii/S0167404821000912>
- Khodjaev, B. H. (2016). Development of historical thinking of students of general education schools by means of modernized didactic support (Doctoral dissertation). Tashkent: [Publisher].
- Kuranov, M. (2008). Reality that we realize. Tashkent: Dukhovnost.
- Lopatin, V. N. (2000). Information security of Russia (Doctor of Law dissertation). St. Petersburg: [Publisher].
- Meulemeester, P. De, Scheers, B., & ... (2020). Differential signaling compromises video information security through AM and FM leakage emissions. IEEE Transactions on <https://ieeexplore.ieee.org/abstract/document/9130107/>
- Ozhegov, S. I. (1990). Dictionary of the Russian language. Moscow: [Publisher].
- Pham, H. C., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. Journal of Information Security and <https://www.sciencedirect.com/science/article/pii/S2214212618302692>
- Sharikov, A. B. (2000). If in doubt, exclude: Children and violence on the screen. [Journal Name], (46), [page numbers if available].
- Smallwood, R. F. (2019). Information governance: Concepts, strategies and best practices. books.google.com.

https://books.google.com/books?hl=en&lr=&id=z3nADwAAQBAJ&oi=fnd&pg=PT11&dq=the+concept+of+information+security&ots=71mDpwC8Qa&sig=ow7oCJgvXMVWGTbtwcLUww4Q_io

- Streltsov, A. A. (2001). The content of the concept "ensuring information security". *Information Society*, (4), [page numbers if available].
- Streltsov, A. A. (2004). Theoretical and methodological bases of the legal provision of the information security of Russia (Doctor of Juridical Sciences dissertation). Moscow: [Publisher].
- Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and* <https://www.sciencedirect.com/science/article/pii/S2214212619306155>
- Toth, A. (2022). Information Security Challenges and Solutions in Smart Nations. *Security-Related Advanced Technologies in Critical* https://doi.org/10.1007/978-94-024-2174-3_10
- Veiga, A. Da, Astakhova, L. V, Botha, A., & Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. *Computers & Security*. <https://www.sciencedirect.com/science/article/pii/S0167404820300018>
- Veiga, A. Da. (2022). Achieving a security culture. *Research Anthology on Business Aspects of* <https://www.igi-global.com/chapter/achieving-a-security-culture/288681>
- Wulf, F., Strahringer, S., & Westner, M. (2019). Information security risks, benefits, and mitigation measures in cloud sourcing. 2019 IEEE 21st Conference <https://ieeexplore.ieee.org/abstract/document/8808060/>
- Zhang, H., Ji, Z., Wang, H., & Wu, W. (2019). Survey on quantum information security. *China Communications*. <https://ieeexplore.ieee.org/abstract/document/9070131/>
- Zhang, P., Schmidt, D. C., White, J., & Dubey, A. (2019). Consensus mechanisms and information security technologies. *Advances in Computers*. <https://www.sciencedirect.com/science/article/pii/S0065245819300245>
- Zhang, Y. (2022). DBSCAN Clustering Algorithm Based on Big Data Is Applied in Network Information Security Detection. *Security and Communication Networks*. <https://doi.org/10.1155/2022/9951609>