

Social and Philosophical Aspects of Information Security

Mukhiba Alimova¹, Asomiddin Khudayberdiev², Muborak Akhmedova³, Miyassar Karimova⁴

^{1,2,3,4}Tashkent Pediatric Medical Institute

E – mail: asomiddin81@inbox.ru

Abstract: The article emphasizes the relevance of information security, the creation of conditions for the need to further expand social measures to ensure information security, the formation of mechanisms and algorithms that determine the behavior of the subject in the information environment, the formation of socio-philosophical foundations of the general theory of information security, and also provides examples, forms of manifestation of information security. The effectiveness of information security in society and information security of youth are analyzed.

Keywords: information Technology; COVID-19; national domain UZ; the Internet; Information Security; information threat, society; confidentiality; social networks; worldview; destructive ideas.

The development of digital technologies in the world has expanded the ability of a person to know the world and himself, and information technologies have opened the way for communication and exchange of ideas in virtual reality. The COVID-19 pandemic not only increases humanity's need for telecommuting, work and communication through information technology, but also creates risks such as depression, confusion and hopelessness for the future. In this situation, the need for states and international organizations is increasing, first of all, in teaching young people how to cope with natural, social and spiritual threats, use knowledge for constructive purposes, and create a safe social space. Therefore, ensuring the safety of technologies in the search, selection and screening of knowledge is becoming increasingly important as a means of protecting against the flow of destructive information that affects the minds of young people.

In Uzbekistan, information technologies are developing in all spheres of society. As the number of users of social networks grows from year to year, ensuring information security has become one of the priorities of state policy. Thus, in 1995 the national first-level domain UZ was registered. If in 2010 in Uzbekistan there were 11 thousand sites regulating the information flow in social networks, then in 2014 their number exceeded 20 thousand, and in 2020 more than 71 thousand active UZ domains are used [1]. These UZ domains allow you to simultaneously monitor the flow of information and analyze the positive and negative views on reforms in Uzbekistan. Since young people are the main capital of the future of Uzbekistan, protecting their worldview from the influence of destructive ideas, fostering the national spirit and patriotism of a modern professional in their social image is a priority of state policy. In this context, “Our key task is to provide conditions for self-realization of youth, to create a barrier to the spread of the “virus” of the ideology of violence” [2], to

further improve information security mechanisms so that young people become the main driver of the development of society; all this confirms the relevance of the study.

A single planetary community is becoming a reality today. Information and knowledge play a special role in ensuring the life of the new civilization, its stability of functioning is determined by the quality of information technology solutions. At the same time, this process has an ambivalent nature: sustainable development of society is already unthinkable without purposeful global informatization, on the one hand, and an increase in the degree of vulnerability of social objects from information impact, on the other. In all spheres of society's life, a class of new types of threats and dangers associated with the use of the latest technological means, which have many variants of their manifestation, has clearly emerged: distortion of information, falsification of reality by virtual worlds, manipulation of people's consciousness, substitution of goals and lifestyle with imposed standards, information wars , etc.

Implementation of the basic principles of information protection at the state and public levels, the practice of popularizing and promoting rights and obligations in the field of information; creation of a scientific and methodological base in the field of information security.

Protection of young people from information threats is achieved through the effective implementation of moral and ethical standards adopted by the state and society, the rules for the safe use of information.

Today, in the education of young people, it is important to further expand social measures aimed at ensuring information security and the formation of mechanisms and algorithms that determine the behavior of the subject in the information environment.

Thus, social measures to ensure information security are a system of application of information technologies and social relations in society, the introduction of technologies adopted and supported by the state, society, community and the individual, aimed at determining the spiritual and moral behavior of an individual.

The particular importance of the process of ensuring protection against information threats and dangers in society shows the need to form the socio-philosophical foundations of the general theory of information security. In turn, social protection measures serve as the basis for the development and popularization of the socio-philosophical concept of information security within the framework of the new scientific theory of information security.

In our opinion, the socio-philosophical foundations make it possible to define, define and develop this theory in a humanistically oriented direction, which ultimately leads to a shift in public consciousness in understanding the content and specifics of information. The solution of these problems will undoubtedly contribute to the formation of ethical rules for social groups and communities, the education of information culture, the safe use of information technologies, the transition of society to a new model of the safe development of civilization.

To implement such a strategy for the survival of mankind, it is necessary to study the prospects of a systemic-futurological nature and the laws of social development, which should be safe development technologies. Therefore, today, in the context of continuing globalization and increasing competition in the information space, a number of scientific studies are being carried out in the field of mechanisms for ensuring the psychological safety of information in the security system. In this regard, it is especially important to find scientific, theoretical and practical solutions to ideological and psychological actions directed

against state sovereignty, independence, territorial integrity and threatening the peaceful life of the population, especially in the information and communication space [2]. The study of the manifestations of information security is determined, first of all, by the novelty of the problem of information security, especially its socio-philosophical component, aimed at ensuring the security of society and the individual, its value preferences in a changing reality. The experience of developed countries in ensuring information security has been studied to some extent, but at present there is no consistent and systematic research. Therefore, this study is important for understanding the specifics of information security and its impact on the further development of society. Theories about the development of an informed society show that researchers have not criticized the opportunities that information technology offers. Consequently, the new threats posed by the use of information technology in society, the negative consequences of which caused concern, were practically ignored.

Information security is a stable state of the information environment that ensures its integrity and protection of objects in the presence of adverse internal and external influences based on the awareness of social subjects of their values, needs (vital interests) and development goals. Information security as an important component of national security includes the following areas: ensuring the protection of the information space - it is very important to ensure the priority of national interests; access to a rapidly and steadily developing global information environment; ensuring the safety of the cultural gene pool of humanity in the context of globalization and so on

Information security threats are actions aimed at the protected object (information sources), aimed at causing harm to the owner of the protected object. These actions can be carried out for the following purposes: Violation of the confidentiality of information, the stored information is of great importance, and its disclosure can cause great harm to the owner of the information. Violation of the integrity of information (partially or completely) is considered close to the threat of its disclosure, but the damage caused by it significantly exceeds the damage to the confidentiality of information.

Important objects of information security are the general values of society (health, well-being, values of a micro-community - family, friends, relatives and social interests) - values accepted and understood in society and reflected in their individual consciousness. The main factor in the construction of information security systems and information systems is ethical measures, since the quality of the security system is determined by the professional level and personal characteristics of a person. In the process of ensuring security, moral and ethical standards serve as a guideline for the safe use of information technologies, in turn, information culture reflects the level of development of individual abilities and determines the quality of its activities. As a result, information security is based on the responsible and ethical behavior of a social subject.

In the field of information security, information ethics sets new principles. The principle of freedom is responsible for ensuring maximum access to information for each member of the information community, overcoming political, economic and other restrictions and discrimination, the problem of such development and solutions. The principle of completeness and integrity of information indicates the need to address the issues of protecting reliability and consistency in the process of storing and transmitting information, such as ensuring the quality of information in global change search systems. The principle of

confidentiality is aimed at solving the issues of protecting personal data from disclosure, loss of confidentiality and changes in information in the course of the activities of informants and manufacturers of databases and data banks in the information community. The principle of responsibility should establish important guiding principles in the process of supporting information technology and ethically regulate the professional activities of professionals.

The protection of information security, human rights and fundamental freedoms, which are the primary concern of information ethics, should not depend on the consequences of the use of information and communication technologies. They represent a certain moral minimum that sets the direction for the future development of society. Information ethics is able to regulate the development of information technologies, ensure their social content and exclude anti-humanistic use.

Legal and ethical norms are a special coordinating mechanism in the field of information security of an individual, society, and the state, which determines the behavior of a social subject in the application of information technologies and the formation of public relations in the social sphere. This mechanism of moral regulation is necessary in order to unite in the public consciousness a set of duties and rights, to awaken a sense of responsibility and respect for these social norms. Its effective functioning in the information society is associated with the improvement of existing legislation by ensuring a balance of technical, ethical, cultural and other aspects, as well as with the study and development of self-regulation in modern society through ethical codes.

Social measures to ensure information security are a multi-level system of methods and technologies adopted and supported by the state, society, community and individual, aimed at the formation and approval of a mechanism for regulating social norms. Social measures should serve as the basis for the development and popularization of the socio-philosophical concept of information security within the framework of the new scientific theory of information security.

Information security covers the following areas: ensuring the protection of the information space, which contributes to the fair distribution of its goods and resources; promoting the development of a sustainable global information environment; ensuring the state of protection of the cultural gene pool of humanity in the context of globalization. Indeed, at the present stage of development of society, effective information security allows us to solve important issues of almost all types of national security.

Information security is an important component of the national security system, and ensuring global security depends on the successful solution of problems in this area. In turn, the process of ensuring information security is an important component of it, along with continuous, complex, socio-cultural aspects, as well as legal, organizational and technical means and methods. The study of the work of the main measures for protecting information led to the conclusion that it is impossible to build a protection system only on technical means, first of all, the strength of the security system is determined by the professionalism and personal qualities of each team member

The solution of information security problems is mainly associated with the loss of humanistic moral values, ideas and moral subordination to political and ideological interests, and information ethics forms its principles: the principle of access to information, the principle of completeness and integrity of information, the principle of confidentiality and

responsibility. These principles of information ethics provide an ethical basis for ensuring the activities of modern society in the field of information security in order to achieve examples of protection of ethics, fairness and moral values in the application of information technology and social relations. The principles of information ethics are reflected in the UN Universal Declaration of Human Rights, which confirms that one of the important tasks of information ethics is to contribute to the development of humanity in society: the main priority of using information technologies in society and public service is the protection of human rights and fundamental freedoms

To achieve this goal, two complementary prerequisites were identified: ensuring the maximum variety of legal content in information networks and ensuring that everyone can own information and information technology. The high speed of new solutions in the field of information technology directly affects human rights and fundamental freedoms, therefore, it is necessary to take them into account when analyzing and programming the possibilities of information technologies to respect universal human values. In this direction, Information Ethics proves its ability to predict and influence the results of the use of information and communication technologies. The study of the prospects for the application of the latest technologies allows us to conclude that in the information society one of the priority directions of state policy is the organization and support of scientific research in the development and implementation of information technologies, as well as the provision of comprehensive analysis and forecasting of the results of their use. Information technologies used by society must have social content and pursue a goal that excludes inhuman use. This article calls for full support for ethical standards in the field of information security, including at the state level, i.e. in the information society, requires a clear mechanism for the adoption and implementation of regulatory legal acts, codes, laws that ensure human rights and freedoms.

In the context of constantly growing domestic and international legal requirements for safety, compliance with these legal norms is becoming an urgent task of modern society. As a result, the information society, within the framework of the adopted information security model, should develop a state strategy for the development and application of information technologies, including the identification of key priorities for social development and the creation of mechanisms for legal coordination. Comprehensive study, taking into account technical, ethical, cultural and other aspects, is an important factor in this process.

At the present stage of the formation and development of the information society, the informatization process is global, all-encompassing, penetrating into all spheres of public life. It turns into one of the main factors of social development and largely characterizes modern social dynamics. Thanks to the process of informatization, systemic changes take place in society, in accordance with which all segments of society and each person are included in the global information space, thus becoming elements of the global information system and, accordingly, more or less dependent on it. The specified information dependence concerns the whole world as a whole, all states and people participating in the process of production, storage and use of information in the course of information exchange and information interaction. As B. Primov noted, “the information society is still the newest civilization in the history of mankind, the main product of which is information and thinking. Information transmitted through contemplation should enrich a person spiritually and morally and serve

reason for the good. It is noteworthy that many of the richest people in the world raise money precisely because of their intelligence. It is not hard to imagine that billions of dollars circulate every day and night through the collection, processing and dissemination of information. The increase in the flow of information led to the introduction of advertising for the products of large enterprises and firms, attracting visitors to a site with an unlimited amount of information via the Internet, owners of "artificial intelligence" and "intellectual property" Microsoft (Bill Gates), Google (Larry Page and Sergey Brin), Founders Facebook (Mark Zuckerberg), Apple (Steve Jobs), Telegram and V Kontakte (Pavel Durov) and others as billionaires "[4].

Information interaction has already become a planetary factor, giving rise to a number of social transformations and introducing into the system of social relations such processes and qualities as information wars, information weapons, information terrorism, information crime and information security. Modern social practices show that social development based on global informatization gives rise to qualitatively new challenges, threats and risks of information security. This circumstance makes information security research relevant. The fact that under the influence of global informatization the social conditions of a person's existence have changed, which is reflected in the formation of a new culture - information, is also actualizing the appeal to the topic of information security of a person. This entailed the transformation of sociocultural values, forms of socialization, motivation of social activity, the content of social roles and social statuses, etc. The human environment has changed, turning into an information environment, and the person himself has also changed - an element of the information environment, more and more acquiring the characteristics of the species "Homo informaticus". Aggressive information environment, overflowing and littered with various, including inaccurate and malicious information, is today an urgent threat to the information security of a person, and therefore, his private information space is violated, an unauthorized invasion of the personal information world is carried out: mass media, propaganda and advertising frankly manipulate a person's consciousness, and information wars make him an object of information aggression. The dependence of a person of the type "Homo informaticus" on global information resources is increasing, which is expressed in Internet addiction, gambling addiction, dependence on the quality and reliability of the information in demand.

Changes in the socio-cultural state of a person's life, changes in his social values and information pressure have complex and contradictory social consequences, including the atomization of social relations, the separation of the individual from the social essence, violation of the right to timely and necessary access to information. All these situations characterize the growing threats to human information security and make the study of information problems, threats and risks a very urgent theoretical and socio-practical problem. From the point of view of disciplinary analysis, the main information that threatens the information security of a person is the global information environment, which has become the dominant development of human society, which:

- a) prevails over all other prerequisites and is full of aggressive, unreliable and even harmful information;
- b) generates global and local information wars and uses information weapons against humans;

- c) carries out informational manipulation of individual and public consciousness at all levels;
- d) creates the conditions for the global struggle for information, introducing aggression and confrontation into the trends of information interaction instead of the ideas of solidarity and partnership;
- e) fights for information, which is expressed in unauthorized intrusions into a person's personal information space, into his inner world using his private information for illegal purposes;
- f) promotes the generation of various informational mythologemes and virtual reality that replaces social reality;
- g) creates conditions for the illegal use of information and the mass dissemination of unreliable, false and even provocative information.

Interdisciplinary methodological analysis goes beyond the limited approach of various specific disciplines to the problem of information security, as it does the following:

- a) consider the interaction of information in modern society in the following two planes: as a subject-object and as a subject-subject interaction, the first type concerns the consumption and use of information, the second type - interactions between information subjects;
- b) integration on a global scale and integration of the diversity of personal and social roles and values of people and the universalization of new cultural values of the information society - information values;
- c) interpret the problem of human information security as a humanitarian problem, i.e. as a problem of information health of society.

The main principles of transdisciplinary methodology as a single concept characterizing the basic research matrix for analyzing human information security are:

- the principle of compatibility, according to which the formation of a basic concept (information security of a person in the information age) is based on identifying a variety of systemic connections of all structural and functional components;
- personal, socio-psychological, socio-group, social, social and civic life in the information age;
- the principle of development, according to which information security of a person in the information age is a systemic quality capable of self-development, including vectors of social dynamics and one of the most important elements of this dynamics;
- the systemic principle of integrity, according to which in the modern information age, human information security is an integral systemic quality with a set of necessary properties and qualities;
- multifactorial and multifaceted information, according to which, in the information age, a person's information security is reflected in the general synthetic unity of individual, personal, socio-psychological, professionally active, spiritual and creative, moral, aesthetic, social group, social, civil and civic parameters.

In the information society, a completely new social phenomenon arises - the globalization of a person's everyday life, which ceases to be personal and intimate, internally closed, closed on the individual, personal-individual, caste-group, class-professional, in accordance with which human everyday life is expressed in social and information practices in the form of social networks (Instagram, Facebook), the blogosphere (Live Journal), thanks to which individual and private information becomes global and is the information property of users

who have access to the information universe; this leads to the fact that the everyday individual in his supposedly individual-personal qualities loses his individuality, becomes massive, averaged as an actor and user of information resources, as an agent of information exchange, information interaction and satisfaction of his information needs and interests, which almost completely destroys personal protective information barriers and creates threats to its information security.

To achieve the effectiveness of information security in society, it is necessary to pay special attention to solving the following tasks:

- at the information and social level - the creation of an information environment;
- providing negative, destructive and non-aggressive information to people as part of the information society;
- information at the level of civilization - the creation of social and civilizational conditions, overcoming the dominant tendencies of social and personal alienation, retreat, individualization and consumer values;
- creation of favorable conditions for the development of social solidarity, social equality, social dialogue between social institutions and people;
- at the information and cultural level - the development of an information culture that promotes self-development and self-improvement of a person and society;
- information at the legal level - the creation of a law on information, which protects information rights and freedoms of each participant in cooperation in the field of information;
- information at the ontological level - a socio-philosophical understanding of threats to destroy the boundaries of social reality and replace it with virtual pseudo-reality;
- at the psychological level of information - overcoming information tension, information phobias and information dependence;
- creation of conditions for compliance with information hygiene and information ecology at the information and environmental level of information health of society;
- principles of information ethics and information law, reflecting the existing norms of information ethics and information law, along with the priority principles of the information society, things that increase the information interests of a person and information values.

These principles can be fully applied to create a stable, non-aggressive, positive information environment, overcome the threats of the globalizing information world, forecast, forecast and manage the threats of the information revolution.

The final conclusion concerns the information health of society, which is a socio-philosophical concept that characterizes the most important conditions for harmonizing information interests and information needs of the state, society and a person, which is the basis of human information security and is implemented at the following levels:

- at the information and social level - the creation of an information environment, which, as a part of the information society, is not negative, destructive and aggressive towards a person;
- at the information and civilizational level - the creation of social and civilizational conditions overcoming the tendencies of social and personal alienation, atomization, individualization and domination of consumer values;
- creation of conducive prerequisites for social solidarization, social equal partnership, development of social dialogue between social institutions and people;

- at the information and cultural level - the development of information culture, contributing to self-development and self-improvement of man and society;
- at the information and legal level - the creation of information law that protects information rights and freedoms of each actor of information interaction;
- at the information and ontological level - social and philosophical understanding of the threats of blurring the boundaries of social reality and its substitution with virtual pseudo-reality;
- at the informational-psychological level - overcoming informational stresses, informational phobias and informational dependencies;
- at the information and environmental level of information health of society - creating conditions for compliance with information hygiene and information ecology;
- at the information and technological level - the creation of effective social control over the introduction of information technologies directed against a person, over the development of malicious forms of software, the use of which through the worldwide network significantly lowers the level of information security of a person.

Research prospects of this topical topic are associated with further explication of the levels of information health of society and the development of practical recommendations that would help to fully implement the developed socio-philosophical concepts in practice. This should find its expression in the development of social technologies that really ensure information security of a person in the context of the challenges and threats of the information age.

References

- [1] The number of sites registered in the national domain UZ exceeded 71,000. <https://www.xs.uz>.
- [2] Mirziyoev Sh.M. Ensuring human interests and rights is the basis of a democratic society // Himself. The consent of our people is the highest value given to our activities. Volume 2 - Tashkent: "Uzbekistan". NMIU. 2018. - 252 p.
- [3] Khaydarov K.A. The mechanism of ensuring the psychological security of information in the defense system (on the example of open sources). Abstract of the dissertation of Doctor of Philosophy (RhD) in Political Science. - Tashkent., 2020. –5 p.
- [4] Primov B.A. The impact of the acceleration of the flow of information on the spiritual and moral education of young people (socio-philosophical analysis). Abstract of the dissertation for the degree of Doctor of Philosophy (PhD) in Philosophy. –Tashkent: 2020. –14 p.
- [5] National Database of Legislation, 22.11.2018, No. 07/18/4024/2200.
- [6] Otamuratov S. Globalization and national-spiritual security. (Political and philosophical analysis) - Tashkent.: "Uzbekistan", 2013.
- [7] Muhammad Amin Yahyo. Protection from Internet threats. - Tashkent. 2016. Movarounnahr. - 295 p.
- [8] Muminov A. Uzbekistan: Towards an Informed Society. –Tashkent., “Turonzaminziyo”, 2013.

- [9] Mamarasulov B. Issues of information security of youth in the process of globalization // "Current issues of ideological and ideological education of students." Resp. scientific conference. –Samarkand. SamISI. 2017. April 28-29. –96-98 p.
- [10] Manoylo A.V., Petrenko A.I., Frolov D.B. Государственная информационная политика в условиях информационно-психологической войны. –Moscow .: Goryachaya liniya - Telekom. 2006, –p. 203.
- [11] Masuda Y. Informationsionnoe obshchestvo as postindustrialnoe obshchestvo. Moscow., 1981.
- [12] Toychiev B.T. Informational aspect of the development of ecopolitic culture. Social philosophy. - Tashkent. NUUz 2015, –p.97-107.
- [13] Yuldashev S.U. (2019) The role of Socio-Cultural Technologies in society. Scientifig Bulletin of Namangan State University, 1(10), 187-192.
- [14] Yuldashev S.U. (2020) Socio-Cultural Technologies in Uzbekistan: History and Now. International Journalof Progressive Sciences Technologies, 18 (1), 171-173.
- [15] Khudayberdiev A.K. (2021) Problems of information security of students. Scientifig Bulletin of Namangan State University, (2), 188-192.