RUDN Journal of Sociology. ISSN 2313-2272 (print), ISSN 2408-8897 (online) **2023 Vol. 23 No. 3 590–599**
Вестник РУДН. Серия: СОЦИОЛОГИЯ http://journals.rudn.ru/sociology

СОЦИОЛОГИЧЕСКИЙ ЛЕКТОРИЙ

SOCIOLOGICAL LECTURES

DOI: 10.22363/2313-2272-2023-23-3-590-599
EDN: VVHSAG

Personal information security as a social problem*

V.A. Tsvyk[1], I.V. Tsvyk[1,2]

[1]RUDN University,
Miklukho-Maklaya St., 6, Moscow, 117198, Russia

[2]Moscow Aviation Institute (National Research University),
Volokolamskoe Shosse, 4, Moscow, 125993, Russia

(e-mail: tsvyk-va@rudn.ru; tsvykirina@mail.ru)

Abstract. Informatization of society has led to a set of fundamentally new problems that humanity has not faced throughout the history of its development. These are the challenges of ensuring the information security of man, society, the state and the entire biosphere of our planet. The article considers the key information security issues of the contemporary world. The authors focus on the nature and essence of information, analyze the concept of information security in a wider and narrower interpretations. They argue that the practices of applying information technologies without ensuring the necessary information security significantly increase the likelihood of information threats, primarily the information inequality, the possibility of manipulations, cyber illnesses, computer crimes, information warfare, etc. Artificial intelligence is one of the key elements of the information age, which is already able to analyze, process and classify huge volumes of rapidly changing and extremely heterogeneous data; thus, the widespread use of artificial intelligence technologies becomes an essential factor in ensuring information security. Artificial intelligence can facilitate the free exchange of information, but it can also be used to spread disinformation and fake news. At the same time, the content moderation for information hygiene purposes can be based on the artificial intelligence algorithms. Thus, artificial intelligence technologies can and should serve as a means of ensuring personal information security. This means that security measures must be comprehensive and include not only instrumental and technological but also ideological and cultural measures — educational in nature, providing the appropriate orientation of the individual.

Key words: information; information security; computer security; information technology; information threats; information inequality; information warfare; artificial intelligence; fake news; information hygiene

---

*© V.A. Tsvyk, I.V. Tsvyk, 2023
The article was submitted on 05.03.2023. The article was accepted on 15.06.2023.

The contemporary society is characterized by an ever-increasing rate of informatization and virtualization, which determines the development of a special, informational consciousness based on the wider use of the benefits of the current scientific-technological transformations unprecedented for the history of mankind. The scale of informatization and the role of the information sector in the economy are increasing, networks and means of communication are rapidly developing, the way of people's life is changing in the new information environment, and professional activities are being informatized [15. P. 132]. Today, there is no doubt that the 'digital revolution' has significantly affected all spheres of society.

However, it would be a serious mistake to consider the prospects for the development of the electronic-digital society only in romantic-glowing colors. Globalization of informatization processes has aggravated many social problems, for instance, those related to intellectual property. Other serious problems of the contemporary world are the increasing number of computer crimes, digital inequality, the strengthening remote component of socialization and social communication, social dehumanization and personal alienation. The most important consequence of the information revolution in the contemporary society is information security, which is determined by the fact that today many of the most important interests of man, society and the state depend on the state of the information sphere surrounding them. The expansion of information technologies sphere is an important factor for the economic development and for improving the functioning of public and state institutions; however, at the same, this expansion creates new information threats. The new, digital world constitutes new challenges for researchers of the informatization of society. Opportunities for the cross-border circulation of information are increasingly used to achieve geopolitical and military-political, terrorist, extremist, criminal and other unlawful goals that contradict the international law to the detriment of international security and strategic stability. Moreover, the very use of information technologies without ensuring information security increases the likelihood of information threats.

Information and information security: nature and essence

One of the significant methodological problems in ensuring the personal information security in the contemporary society is the understanding of the nature and essence of information, especially in the scientific, philosophical perspective. Today information is the main research object of many disciplines; however, the current level of the development of scientific knowledge does not allow for an accurate and complete definition of information, and its conceptual field expands and deepens with the development of our understanding of the world. In addition, information is a multifaceted phenomenon that manifests its properties differently in different situations. The diversity and multidimensionality of the concept of information allows to define it as a general scientific category, as a universal substance. One

of the most general definitions of this concept was introduced about fifty years ago by V.M. Glushkov: "Information, in its most general sense, is a measure of the heterogeneity of the distribution of matter and energy in space and time, a measure of the changes that accompany all processes taking place in the world" [8. P. 57]. We can expand this definition from the standpoint of the contemporary level of the scientific development with reference to K.K. Colin: "Information in the broad sense of this term is an objective property of reality, which is manifested in the heterogeneity (asymmetry) of the distribution of matter and energy in space and time, in the unevenness of all processes occurring in the world of living and inanimate nature, as well as in human society and consciousness" [6. P. 62]. Therefore, the main features of information are as follows: ideality, continuity, inexhaustibility, mass, transformability, versatility, the ability to compress and transport at high speed, quality (adequacy and reliability), completeness, accessibility, relevance, etc.

Thus, information is a complex, multifaceted comprehensive phenomenon, its specific sides and characteristics are studied by many sciences which, being independent, develop in inextricable unity, complementing and enriching each other. All this indicates that the concept of information is ambiguous, and the variety of its interpretations reflects the very complex nature of the real world, making it difficult to work out solutions to the problem of ensuring information security of the individual in the contemporary world.

Security in its broadest sense is the prevention and avoidance of threats to key values and interests. When defining security, the emphasis is often made on the availability of funds and organizational measures, institutions, arrangements with partners, etc. However, the whole complex of ensuring security depends on the nature and scale of threats; therefore, the concept of security implies threats and protection against them. Depending on the object being threatened and in need of protection, we can identify 'human security' — in its individual quality, 'security of a group' — for example, of the ethnic or religious group, 'public safety', 'national security' of the state, 'regional security' or 'collective security' of groups of states that constitute a region or union, and, finally, 'international security' or 'global security' of the world community. According to the functional type of threats and means of protection against them, security can be military, economic, political, environmental, cultural, informational, etc. Information is generally understood as the state of security of the information environment of the society, which ensured its stability and development in the interests of citizens, organizations, and the state.

Ensuring information security in contemporary Russia

In recent decades, the society has become aware of the relationship between the state of the information environment of the society and the possibilities of achieving the most important goals and interests of the person, state and society. However, many states, including Russia, have already developed and adopted their national doctrines in the field of information security as the basis of their state

policy. In addition, already in 1998, Russia initiated the development of the draft international concept of information security in order to ensure the coordination of efforts of all countries of the world community.

One of the first Russian laws on information security is the Federal Law "On Information, Information Technologies and the Protection of Information" of July 27, 2006 [1]. "It gives basic definitions, outlines areas in which legislation should be developed in this area, regulates relations determined by: 1) the right to search, receive, transmit, produce and disseminate information; 2) the application of information technologies; 3) the protection of information. The law also provides definitions of the basic concepts in the field of information security. Thus, information technologies are defined as processes, methods for searching, collecting, storing, processing, providing, disseminating information and methods for ensuring such processes; information system is defined as a set of data in databases and the information technologies and technical means providing it; information holder is defined as a person independently creating or obtaining information on the basis of a law or an agreement, or the right to allow or restrict access to information by any criteria, etc." [19. P. 43].

The set of the official interpretations of the goals, objectives, principles and main directions in ensuring information security in Russia is presented in the National Security Strategy of the Russian Federation (2015) and the Doctrine of Information Security of the Russian Federation (2016). The National Security Strategy considers information security as an integral part of Russia's national security, since "the growing confrontation in the global information space is increasingly influenced by the desire of some countries to use information and communication technologies to achieve their geopolitical goals, including by manipulating public consciousness and falsifying history… New forms of illegal activity appear, in particular with the use of information, communication and high technologies" [2]. In the Doctrine of Information Security, information security is defined as "the state of protection of the individual, society and the state from internal and external information threats, which ensures the realization of constitutional rights and freedoms of citizens, high quality and standards of living, sovereignty, territorial integrity and sustainable social-economic development of the Russian Federation, defense and security of the state" [3].

Key problems in ensuring the personal information security

Many challenges in ensuring information security are common to all people of our planet, i.e., these are global problems. First, the danger of deformation of traditional cultures under the influence of global informatization which contributes to the wider distribution of mass culture. Thus, spiritual values of traditional cultures are being destroyed in many countries of the world and substituted by new values of the consumer society, which is extremely dangerous for the future of our civilization. Second, the need to ensure the energy-information security of the

planet's biosphere under the rapidly increasing tensions in energy and information fields of the anthropogenic nature [7. P. 38]. These fields can have devastating effects on the gene pool of the biosphere in general and on the development processes of living organisms and plants; although the permissible level of this effect to humans is still unknown. Third, information inequality — the problem of ensuring real equality in the access and use of new information technologies. This problem is rooted not only in economic, instrumental or technological factors related to the certain complexity of ensuring all users' access to the information resources, but also in personal psychological factors: linguistic competence, education, information competence, and motivation to increasing one's knowledge and learning. If the person does not want to be an active member of the information society, no technology would help him.

Forth, the development of global networks of information communication creates wider opportunities for influencing and manipulating the public consciousness. Today researchers comprehensively study various technologies for manipulating the mass consciousness — from rather innocuous, such as, for example, substitution technology, reversal of accents, ironization, degeneration, desymbolization, etc., to the extremely dangerous technologies of overt information aggression and information war. The methods and means of information warfare are already well developed in both theoretical and applied aspects. Information wars have become a very common and effective way of confrontation in the political, economic and cultural fields. In the future, due to the development of the means and institutions of the information society, information wars will certainly become even more widespread both locally and globally.

Fifth and the fundamentally new danger to the individual in the information society is the so-called cyber disease, i.e., the psychological dependence on the mass media — from television to the Internet — and computer games. One of the extreme manifestations of such dependence is the virtualization of consciousness, when the person becomes unable to distinguish between objective reality and virtual reality. This psychological phenomenon is increasingly manifested in the information society — when real physical objects, processes and phenomena are replaced by their virtual images similar to the displays of objective reality. Social communication is also virtualized, and communication in social networks replaces real, live communication. Moreover, the anonymity of such network communications makes it possible to replace the true personality with a certain invented surrogate, which can lead to a loss of personal identity.

The proliferation of the functionally powerful automated information systems leads to significant changes in the field of mass communication and information dissemination. On the one hand, the growing possibilities of using data and computer technologies to solve research tasks can make information workers more efficient. On the other hand, automation of information flows, automated writing of news without human participation or control is often hidden from the

consumer of information — reader or listener. In creating and distributing media content, analytical tasks and decision-making functions are increasingly delegated to complex algorithms, which raises the questions of responsibility, transparency and copyright. The problem of liability for the dissemination of low-quality or untrue information is hard to solve when the data was produced with the use of algorithms, for example, in the case of defamation.

Thus, the information society seems to be very vulnerable to destructive information influences, which significantly exacerbated the problem of ensuring information security and confirms its global nature.

Artificial intelligence and personal information security

Artificial intelligence is one of the key elements of the information age, in the era of technological convergence, which is associated with significant consequences for humans, culture, society, and the environment. Artificial intelligence can analyze, process and classify huge volumes of the rapidly changing and extremely heterogeneous data, which makes the widespread use of artificial intelligence technologies an essential factor in ensuring information security. "Artificial intelligence is playing an increasingly important role in the processing, structuring and provision of information. Automated journalism and algorithmic news in social networks are just some examples of this trend, which raises issues of access to information, disinformation, discrimination, freedom of expression, privacy, data protection, information literacy and information hygiene. The widespread use of artificial intelligence technologies also creates new digital and information gaps between countries and between social groups" [16. P. 60].

Journalism based on artificial intelligence raises issues of subjectivity and copyright, transparency and reliability of disseminated information, responsibility for the dissemination of unreliable or even initially false information. The problem of responsibility — both legal and moral — is a part of the situation when information materials are prepared with the help of artificial intelligence systems. Problems of transparency and reliability are due to the situation when users do not understand or cannot understand what content was created by the machine, from what sources it came and how reliable or false this content is. The issue of copyright is no less important, since content created by artificial intelligence depends less on personal contribution, which leads to the discussions on what part of responsibility for copyright compliance the algorithms should take in one form or another.

Artificial intelligence technologies can facilitate the free exchange of information, but they can also be used to spread disinformation, 'fake news'. Algorithms, which were originally created to avoid the inherent personal political bias when deciding which content to post on social networks in the most visible places, can be intentionally used to disseminate fabricated, manipulative or divisive information among specific target groups. In some cases, such content may include information fraudulently framed as news reports or forms of emotional propaganda

[4. P. 45]. All this can negatively affect both the norms of civilized and substantive discussion and the individual. Algorithms of social networks can aggravate the polarization of opinions, amplifying and multiplying the emotional effect with the help of 'endorsements', 'forwarding links', 'repeating messages', etc. [9]. Some large companies that own social networks have realized the need to solve this problem with the participation of many stakeholders, including civil society and government regulators, but the ways out of this situation are still not clear. One of the ways can be the application of the principles of law, openness, accessibility for all, and the participation of many stakeholders. Content moderation can also be a justified decision to ensure personal information security, since it helps to avoid the spread of misinformation, materials inciting violence, hatred and discrimination and to prevent aggression in interpersonal communication. Content moderation and filtering can be provided by both humans and artificial intelligence algorithms.

Computer security: concept and essence

Today the term 'computer security' or 'information security' is used in both wider and narrower senses. Computer is exposed to only a few risks if it is not connected to other computers. In recent decades, the share of computer networks (especially the Internet) has grown significantly, so today the term 'computer security' means problems associated with the network use of computers and their resources. One of such problems is the protection of personal data, which has a number of aspects — technological and organizational — related to restricting access to the computer and the data of unauthorized users, and to the general system for organizing data transmission and storage. In general, the problem of protecting information from computer malicious viruses and physical unauthorized access to classified information is successfully solved today by improving antivirus programs and computer software.

Computer security systems protect information from a wide range of threats to ensure confidence in business, minimize damage, maximize return on investment and realize potential business opportunities. Regardless of the form of information and means of its distribution or storage, it should always be adequately protected. Computer security mechanisms provide confidentiality (access to information only for authorized users), integrity (reliability and completeness of information and methods for its processing) and accessibility (access to information and related assets for authorized users as needed).

Other important components the computer security professionals pay great attention to are access control and strict compliance. Access control implies not only that the user has access only to available resources and services, but also that he has access to the resources he legitimately expects. As for the strict fulfillment of obligations, it implies the restrictions for users in order to fight against computer crimes (attempts to prevent, detect attacks) and confidentiality (anonymity) in cyberspace.

Thus, the above analysis of the main features of the new information reality shows that the changes taking place in the information sphere determine radical transformations in both social-economic structures and processes of personality formation and lifestyle. Under the development of information and communication technologies, information security issues go beyond the traditional questions of security and affect absolutely all spheres of life. To solve global problems of information security, humanity needs a new system of legal relations in the information sphere, a new information culture and a relevant information ethics. However, the most important thing is to admit both the very existence of these problems and the need for their urgent solution by civilized methods. Information crimes, information aggression and information warfare are no longer metaphors for futurologists, but rather scientific terms that indicate very specific new phenomena in our social life. Therefore, the measures to ensure information security should be comprehensive and combine instrumental-technological and ideological-cultural-educational approaches [21. P. 123]. The new information environment should follow certain philosophical-axiological priorities in order to change the basic value characteristics of the information society.

References

1. Federalny zakon "Ob informatsii, informatsionnyh texnologiyah i o zashchite informatii" No. 149–FZ ot 27 iyulya 2006 goda [Federal Law "On Information, Information Technologies and Information Protection" No. 149–FZ of July 27, 2006]. URL: https://rg.ru/2006/07/29/informacia-dok.html. (In Russ.).
2. Strategiya natsionalnoj bezopasnosti Rossijskoj Federatsii. Utverzhdena Ukazom Prezidenta Rossijskoj Federatsii ot 31 dekabrya 2015 goda No. 683 [National Security Strategy of the Russian Federation as approved by the Decree of the President of the Russian Federation of December 31, 2015 No. 683]. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html. (In Russ.).
3. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii. Utverzhdena Ukazom Prezidenta Rossijskoj Federatsii ot 5 dekabrya 2016 g. No. 646 [Information Security Doctrine of the Russian Federation as approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. (In Russ.).
4. Ashley K.D. *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge; 2017.
5. Boden M.A. *AI: Its Nature and Future.* Oxford; 2016.
6. Colin K.K. Filosofiya informatsii: struktura realnosti i fenomen informatsii [Philosophy of information: The structure of reality and the phenomenon of information]. *Metafizika*. 2013; 4 (10). (In Russ.).
7. Colin K.K. *Filosofskie problemy informatiki* [Philosophical Issues of Computer Science]. Moscow; 2010. (In Russ.).
8. Glushkov V.M. O kibernetike kak nauke [On cybernetics as a science]. *Kibernetika, myshlenie, zhizn*. Moscow; 1964. (In Russ.).
9. Frankish K., Ramsey W.M. *The Cambridge Handbook of Artificial Intelligence*. Cambridge; 2014.
10. *Istoriya i filosofiya nauki* [History and Philosophy of Science)]. L.E. Motorina, I.V. Tsvyk (Eds.). Moscow; 2023. (In Russ.).

11. Kazantsev A.A. *Rasshirenie problematiki bezopasnosti v politike Rossii: sekyuterizatsiya, biopolitika i novye administrativnye praktiki* [Expanding the Security Issues in Russia's Politics: Securitization, Biopolitics and New Administrative Practices]. Moscow; 2011. (In Russ.).
12. Kvon D.A., Pavlova T.P., Tsvyk I.V. *Filosofiya i metodologiya iskusstvennogo intellekta* [Philosophy and Methodology of Artificial Intelligence]. Moscow; 2021. (In Russ.).
13. *Nauchno-tekhnichesky progress i eticheskaya paradigma XXI veka*. [Scientific-Technological Progress and Ethical Paradigm of the 21st Century]. V.A. Tsvyk (Ed.). Moscow; 2018. (In Russ.).
14. Payne K. Artificial intelligence: A revolution in strategic affairs? *Survival.* 2018; 60 (5).
15. Tsvyk V.A. *Professionalnaya etika: osnovy obshchej teorii* [Professional Ethics: Foundations of General Theory]. Moscow; 2020. (In Russ.).
16. Tsvyk V.A., Tsvyk I.V. Sotsialnye problemy razvitiya i primeneniya iskusstvennogo intellekta [Social issues in the development and use of artificial intelligence]. *RUDN Journal of Sociology.* 2022; 22 (1). (In Russ.).
17. Tsvyk V.A., Tsvyk I.V. Professional development in information society: Challenges and prospects. *RUDN Journal of Sociology.* 2018; 18 (3).
18. Tsvyk V.A., Tsvyk I.V. Moral education of youth in the information society. *Voprosy Filosofii.* 2020; 4. (In Russ.).
19. Tsvyk V.A., Tsvyk I.V. Informatsionnaya bezopasnost v sovremennom obshchestve: ponyatie, osnovnye problemy [Information security in the contemporary society: Concept and main issues]. *Filosofskoe Obrazovanie.* 2017; 1. (In Russ.).
20. Vernon D. *Artificial Cognitive Systems: A Primer.* Cambridge; 2014.
21. *Vospitanie molodezhi: problema formirovaniya tsennostej v usloviyah informatsionnogo obshhestva* [Education of the Youth: Formation of Values in Information Society]. V.A. Tsvyk (Ed.). Moscow; 2020. (In Russ.).

DOI: 10.22363/2313-2272-2023-23-3-590-599
EDN: VVHSAG

Информационная безопасность личности как социальная проблема*

В.А. Цвык[1], И.В. Цвык[1,2]

[1]Российский университет дружбы народов,
ул. Миклухо-Маклая, 6, Москва, 117198, Россия

[1,2]Московский авиационный институт (национальный исследовательский университет),
Волоколамское шоссе, 4, Москва, 125993, Россия

(e-mail: tsvyk-va@rudn.ru; tsvykirina@mail.ru)

Аннотация. Статья посвящена проблеме обеспечения информационной безопасности в современном мире. Авторы рассматривают природу и сущность информации, анализируют понятие информационной безопасности в широком и узком смысле. Опираясь на научные и прикладные исследования, авторы утверждают, что нынешняя практика внедрения

*© Цвык В.А., Цвык И.В., 2023
Статья поступила 05.03.2023 г. Статья принята к публикации 15.06.2023 г.

информационных технологий без обязательной увязки с обеспечением информационной безопасности существенно повышает вероятность проявления прежних и появления новых информационных угроз, среди которых особенно значимы такие проблемы, как нарастающее информационное/цифровое неравенство, возможности манипуляции общественным сознанием, киберболезни (компьютерная зависимость и др.), компьютерная преступность (киберпреступность), информационные войны и др. Искусственный интеллект становится одним из ключевых элементов современной информационной эпохи: он способен анализировать, обрабатывать и классифицировать огромные объемы быстро меняющихся и чрезвычайно разнородных данных, что делает широкое распространение технологии искусственного интеллекта существенный фактором обеспечения информационной безопасности. Искусственный интеллект может способствовать свободному обмену информацией, но может использоваться и с целью распространения дезинформации, так называемых «фальшивых/фейковых» новостей. В то же время, и модерация онлайн и медийного контента в целях информационной безопасности и гигиены также может выполняться с помощью алгоритмов искусственного интеллекта. Таким образом, технологии искусственного интеллекта могут и должны служить средством обеспечения информационной безопасности личности. Авторы делают вывод, что меры по обеспечению информационной безопасности должны быть комплексными и подразумевать не только инструментально-технологические решения, но и воздействия идеологического и культурно-воспитательного характера, направленные на формирование и закрепление соответствующих ценностных ориентаций личности.

Ключевые слова: информация; информационная безопасность; компьютерная безопасность; информационные технологии; информационные угрозы; информационное неравенство; информационные войны; искусственный интеллект; фальшивые новости; информационная гигиена