A systematic approach to personal information security in the context of digitalization of the economy and management

Lyucyena E. Puinko*, and *Elena V*. Tolkacheva

Far-East Institute of management, branch of the Russian Presidential Academy of National Economy and Public Administration (hereinafter RANEPA), Department of mathematical methods and information technologies, Khabarovsk 680000, Russia

Abstract. The digitalization of the economy and the digitalization of management in a modern state imply not only the use of many different technical devices that interact with each other through global and regional communication networks. But also the transformation of sociocultural communication in society; a significant change in the forms and types of interaction of the individual with the participants of the interaction processes: other individuals, state institutions and commercial and non-profit organizations, etc. In the context of such interaction, the complexity of structures and types of communication-the personal space of participants is blurred, the security of the individual in the information field is becoming more and more vulnerable; the mechanisms for protecting the individual in the digital economy and digital management today are imperfect; this is also due to the fact that the study of "information security" and "information threats" today lacks a systematic approach that combines their individual elements into a holistic scientific knowledge – the protection of the individual in the information space of modern society. The purpose of this article was to analyze the possibility of systematization of scientific knowledge on this problem and the possibility of creating the concept of information security of the individual.

1 Prerequisites for a systematic approach to personal information security

In the modern world and in modern science, more and more attention is paid to the information security of the individual, as well as the information security of networks and systems. This is primarily due to the transition from a "post-industrial society" to an "information society". There are also deeper grounds for successful informatization, determined by the nature of system-forming social relations. Thus, the growth in the volume of intellectual production and the quality of management entails the loss of property value in the face of knowledge and information, the ownership rights of which can only be very limited and conditional [1, 2]. The object of ownership, use and disposal of modern

* Corresponding author: lusiena_03@mail.ru

employees of the intellectual sphere is the finished product of their creative activity-knowledge or information. [3]

1.1 Modern processes of globalization and related information security of the individual

The difficulties of the modern study of information security and information threats lie in the "blurred" definitions and concepts of this phenomenon, since the concept of "information security" appeared relatively recently. The end of the XIX – beginning of the XX centuries can be considered as the period of the emergence and formation of information threats, including the use of information, in its either distorted form, or deliberately false information. Moreover, the processes in the field of information security of the XXI century, our days, and the existing types of various information threats today are connected and integrated into the processes of globalization. I.e., the blurring of the concepts of "state", "nation", "national idea", "traditional family", natural rights and freedoms of the individual; rights and freedoms that are organically combined with human nature, and not artificially imposed formations. The processes of globalization are complex in their structure and interrelationships, hence the lack of consistency and a systematic approach to their study. Accordingly, the lack of a system-forming component arose when studying the concepts of "information security" and "information threats".

Modern science is actually very complex, has a complex structure, complex intersections of knowledge areas in various fields. Despite the fact that humanity, as the interaction of modern states and societies, is one; the natural environment in all its diversity exists as a single system, etc. [2] Thus, science, the main properties of which are truth and integrity, according to general opinion, should be considered as a single and consistent system of knowledge [2, 3].

That is why the study of the processes of globalization requires a systematic approach that considers not only certain beneficial elements of this process for narrow social groups, but also the negative aspects of globalization for the family, nationalities, nations, and independent states. Hence, the systematic principle of studying information security and information threats associated with the modern development of humanity, moving from a post-industrial society to an information society.

1.2 Systematization of personal information security knowledge in the context of the modern knowledge system

At the same time, it is necessary to understand that in the conditions of the development of the modern economy and its formation - the "digital economy"; it is impossible to replace the real economic sector, the service sector, including financial. I.e., a healthy economic model is needed, in which the financial sector, as a service sector of the economy, performs its functions to ensure cash flows in the structure of interaction between enterprises, households and the state. The financial sector, primarily as a service sector, cannot be dominant in a healthy economic model. Accordingly, everything related to information security exists systematically to ensure the security of all participants in the economic model.

Here we approach the definition of "personal information security" as one of the basic elements of modern information, social, legal, political and economic systems.

The modern exponential growth of intellectual production, which implies information as an initial resource, processed information necessary for decision – making, as a finished product (or intermediate product), implies the intellectual work of individual workers (individuals), then the production of qualitatively new information by them is the result of

their work. At the same time, we note that the objects of intellectual labor (in fact, "intellectual property") are practically inseparable from the person who produces and uses them. The same concept is claimed by V. A. Rubanov [3]: "This is, to a large extent, the person himself and his abilities, and not an external commodity that can be used by anyone, and in any way. The personal ownership of employees in their unique abilities and the opportunities that open up for the independent creation of a complete intellectual product form a class of intellectuals who occupy a dominant position in the labor market and dictate their own conditions to society. The most important resource is not the labor force of the industrial era, but knowledge as the main object of personal property of the post-industrial era" [3].

In addition to the designated intellectual workers, in modern economic models of economies, there are workers who produce a material product (machine parts, chemicals, clothing, furniture, machine tools, etc.), they are also included in the modern processes of digitalization of the economy (they, as household participants, receive income on bank cards, use contactless payment systems, participate in modern information flows and exchanges, etc.). All individuals, individuals in the modern world interact in the processes of processing their personal data. Taking into account the development of artificial intelligence systems, and other systems (processes) of digitalization; on a daily basis, artificial information systems process data flows that are inherently associated with each individual. An example is the geolocation systems built into modern models of gadgets (smartphones, iPads, iPhones) that track all the routes of their owner, collect, classify, process this information, store it and transmit it. Smart city systems, which include video surveillance and monitoring systems, are also capable of reading, processing, storing, and transmitting information about individuals; other examples can be cited.

At the same time, modern financial institutions put forward proposals for the use of data on the geolocation of their customers for commercial purposes, they intend to "sell" this information to stores, service companies, etc., Moreover, they already do this in an implicit form (for example, helpfully offering products and services of their partners in the online offices of their customers, i.e. those companies that pay for such advertising to banks). Information systems, such as Internet search engines, also include "smart search" and offer targeted advertising to their users. Here we do not give as an example artificial systems of surveillance of the person, which implement criminal structures, but they also implement data collection, similar to geopoisk and the use of intelligent systems.

1.3 Types of information threats to the individual in the modern world

It should be noted that personal data of a person, information as a product of the production of a person, is just one of the aspects of information security and information threats of our time. There are information threats in messengers, social networks; the collection of personal data using artificial intelligence systems in social networks and messengers, for example, about law enforcement officers, which in itself is a threat not only to law enforcement officers and their families, but also to the state law enforcement system. Cybersecurity, as a form of countering cybercrime, is also taken out of the brackets by the authors in this study. Since the issues of cyber threats thirty years ago were reduced to threats to industrial security (industrial espionage) and countering hacker attacks. Modern cyber threats [4, 5, 6], additionally include cyber bullying, phishing, so-called services in the darknet, spying on individuals, penetration of family (personal) secrets, slander on the Internet, the use of social groups in messengers and social networks that carry a terrorist threat, fake online stores, Online fraud, and much more. All these topics cannot be covered in this article.

Some researchers consider information security from the point of view of the use of technical devices [4, 5], the information environment, i.e. as a method of hardware and software data protection [4, 5, 6]. Of course, this approach is one of the basic ones, because digital properties of information, as a form of transmission of commands and data over communication networks, processed by certain network protocols, using software and hardware methods of protecting the transmitted data – all this is relevant and important today from the point of view of the physical and information properties of the information itself and information security. We also note the importance of a systematic approach: in the integration of all spheres of individual life (social, economic, legal, political, religious, etc.).

2 The main aspects of the formalization of the system approach to the information security of the individual in the digital economy

2.1 Scientific aspect of personal information security

The authors distinguish in the study of information security and information threats, as components of information security, a systematic approach associated with such aspects of the study as: scientific, practical, social, legal, economic, and political.

Then, as part of the system of directions for studying information security, we will highlight the risks that exist in several aspects:

So from the point of view of the scientific aspect, this is a weak study of the possibilities of artificial intelligence technologies in assessing the levels of information security of an individual in the context of digitalization of the economy and management in the Khabarovsk Territory. The problem of the prevalence of artificial intelligence and neural networks, the collection of information about geolocation by banks and other commercial organizations.

2.2 Practical aspect of personal information security

According to the practical aspect, the threat can be a high level of crimes and offenses committed against the individual using information channels and technologies. Digitalization of various sectors of the national economy and management carries a number of information risks and threats. These include unauthorized access to information and other cybersecurity threats. Threats are also hidden in the collection of data about their users of various services and services, which is associated with the problem of hidden data collection, when the information needed for some additional, rather than the main functions of the system (the same mobile application) is generated automatically, for example, by tracking geolocation when using bank cards. At the same time, the main risks are associated with the possibility of using artificial intelligence by attackers by bypassing security systems [7, 8].

2 3 Social aspect of personal information security

In the social aspect, this is the social insecurity of the individual. The use of digital interfaces by the population means a kind of replacement of the "analog identification" of the individual with a fully digital one. On the one hand, this is convenient, but on the other hand, it is risky, since there are threats of so-called "identity theft", that is, the commission of full-fledged civil and professional actions on behalf of a particular citizen.

2.4 Legal aspect of personal information security

In the legal aspect, these are blurred outlines in the legal framework of concepts related to" cyber - crimes", crimes and offenses using artificial intelligence; gaps in legislation regarding the information security of the individual, personal information, as an inherently personal subject in information legal relations; the use of these gaps in legislation by financial institutions for profit based on the appropriation and use of information data about individuals (clients of financial institutions).

2.5 Economic aspect of personal information security

From the point of view of the economic aspect, the threat can be the transformation of economic concepts in the field of human resources, human potential, the shifting of the boundaries of the inviolability of personal and personal data, in order to use them by financial institutions; the substitution of the real economy by the financial sector, which acts not as a system of servicing the real sector of the economy (in classical economic theory), but as a superstructure and self-producing economic resource (when money produces money, without the basis of commodity-money turnover). The formation of a trend in economic theory, "human capital" or "human resource", as a means of profit-making, when the humanistic approach to the individual is replaced by a false approach – the individual as a resource for profit-making by companies and corporations.

2.6 Political aspect of personal information security

In the political aspect, threats to the information security of an individual can escalate into tension in society and increase crime in this area. The blurred boundaries of what is permissible in the handling of personal data, the penetration of family and personal secrets by intruders, etc., destroy state institutions, including the institution of the family, which in turn leads to the destruction of state security and state integrity, in the worst forms – this is a civil war (or a war of all against all).

3 Conclusion

According to the authors, it is impractical to consider all these aspects in isolation, since the integrity of the scientific study of "information security" is violated.

The systematic approach to the study of "information security" aims to develop a conceptual model of measures in the field of information security. At the same time, taking into account the considered aspects, the construction of appropriate methods of counteraction and the writing of appropriate algorithms of individual behavior to protect their information space, implies the systematization of existing methods of protection; interaction with law enforcement agencies and public administration in terms of improving the literacy of the population in terms of information security, as well as the use and improvement of public information space approaches at the level of state institutions to counter threats to state security (for example, electronic displays of street advertising, on which individual videos are broadcast, must necessarily have security and encryption devices that prevent intruders from entering the broadcast, the proposed systematic approach in the field of "information security", there is a need to detail measures to counter information threats.

The authors see in the development of such counteraction measures not only instructions for civil servants, or the public in their interaction with the financial sphere and the sphere of online commerce, but above all measures at the family level in terms of

protecting the information security of family members. In this direction, the authors develop conceptual models of child safety, anti-bullying and other measures that are also outside the scope of this article.

The main conclusions of the study " information security»: there is a lack of consistency in the study of "information security" and "information threats"; there are no conceptual models for countering information threats; it is necessary to develop measures and measures to counter information threats not only classified by type, but also considered as an integral system of knowledge.

This work was supported by Far-East Institute of management, branch of the Russian Presidential Academy of National Economy and Public Administration (hereinafter RANEPA), Department of mathematical methods and information technologies, Khabarovsk 680000, Russia.

References

1. Bohme G. Am Ende des Beconschen Zeitalters, Wissenschaft und Gesellschaft [Science and. Society]. No. 3, 129 p. (1992)
2. Gorokhov V. G., Sidorenko A. S. The role of theoretical research in the development of new technologies. №9; Gorokhov V., Lenk H. NanoTechnoScience as a Cluster of the Different Natural and Engineering Theories and Nanoethics // Silicon vs Carbon: Environmental and Biological Risks of Nanobiotechnology, Nanobionics and Hybrid Organic-Silicon Nanodevices. Freiburg/ München: Springer, 2009. P. 190-213. (2009)
3. Rubanov, V. A. Problems of transition to the information society: imperatives for Russia. URL: https://cyberleninka.ru/article/ n/problemy-perehoda-k-informatsionnomuobschestvu-imperativy-dlya-rossii/viewer. (2004)
4. Vladimir A. Tsvyk, Irina V. Tsvyk. Personal Information Security as a Global Problem // URL: https://www.researchgate.net/publication/344758888_Personal_Information_ Security_as_a_Global_Problem. (2020)
5. Tsvyk A.V. Ethics of Political Responsibility in International Relations // Bulletin of the Peoples' Friendship University of Russia. Series: International Relations. -2017. -T. 17. No. 2. -P. 257-264. (2017)
6. Personal Information Security Guide for Family and Friends. Help your family and friends being secure with this printable security guide // URL: https://auth0.com/blog/personal-information-security-identity-guide. (2020)
7. Stephen D. Gantz. IT Audit Drivers / in The Basics of IT Audit, 2014 // URL: https://www.sciencedirect.com/science/article/pii/B97801241715960 00079. (2014)
8. Dariusz Kloza, Nielsvan Dijk, PaulDe Hert / in Smart Grid Security, Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologiesa // URL: https://www.sciencedirect.com/science/article/pii/ B978012802122400002X. (2015)