

*Kurilo A., adjunct candidate of Educational, Scientific and Production Center of the National University of Civil Defense of Ukraine, Kharkiv*

ORCID: 0000-0002-5139-0278

## **SOCIOLOGICAL MONITORING OF PROCESSES OF FORMATION OF PUBLIC MANAGEMENT OF SOCIETY'S INFORMATION SECURITY**

*The article is devoted to the study of the processes of formation of public management of information security of society. Public management of information processes, interests of subjects in the information sphere and protection of these interests are homogeneous elements of the information system. They are closely interconnected, mutually conditioned and interdependent. Therefore, the social management of information processes optimizes the processes of forming the information security of the subject (individual, society, state), the interests of the subjects of the information sphere are regulated by the appropriate management of information processes (from global to local) and are provided with the necessary protection.*

**Keywords:** *information, information security, state information policy, threats to information security, national security, national security strategy.*

**Formulation of the problem.** Public management of information processes, interests of subjects in the information sphere and protection of these interests are homogeneous elements of the information system. Today, in our opinion, there is a noticeable gradual and steady flow of the main problems related to the processes of forming information security of society into the social plane: for example, the technical

part of information security is increasingly complicated by the social causes of the problem.

**Presenting main material.** The theoretical-methodological substantiation of the model of sociological monitoring of the processes of forming the information security of society involves the use of the concept of information security, which is reflected in the Information Security Strategy of Ukraine, in particular, the definition of information security as a component of the national security of Ukraine, the state of protection of state sovereignty, territorial integrity, democratic constitutional system, other vital interests of a person, society and the state, under which the constitutional rights and freedoms of a person to collect, store, use and distribute information, access to reliable and objective information are properly ensured, there is an effective system of protection and countermeasures against harm due to the spread of negative information influences, including the coordinated dissemination of false information, destructive propaganda, other information operations, unauthorized dissemination, use and violation of the integrity of information from limited access [1]. The object of special concern of the society in this sphere is the strengthening of democracy, achievement and maintenance of social harmony, increase of creative activity of the population. According to many scientists, two strategies for ensuring information security are possible. The first is a reaction to the facts (post factum) in cases of an attack on information security. Namely, their detection, analysis of the causes that caused the events, the possibilities of their elimination or weakening of the action, the use of sanctions against offending agents, those who provoke them, etc. The second strategy is a preventive one, focused on predicting the possible appearance of information security violations, deploying countermeasures to prevent or mitigate negative consequences. Both strategies are mutually dependent and complementary. No matter how carefully organized the counteraction and prevention system is, both prerequisites and violations of information security will arise. Therefore, an adequate reaction to them is required. The funds spent on the deployment of preventive actions are an order of magnitude lower than the costs incurred on eliminating the causes and consequences of information security violations.

Indeed, we can agree that the concept of security does not imply total freedom from any danger or threat, because human activity contains elements of creativity, as well as elements of risk, dangers accompanying creative and social processes, revealing the potential for development and improvement of social structures, institutions and processes. At the same time, the possibilities of managing and regulating nature, social life, and technology are always limited. Therefore, a safe strategy is not only the elimination and prevention of danger, but also the painless overcoming of dangerous situations, which is directly related to information security. Hence, the need to turn to sociological monitoring is caused by the complex nature of the phenomenon information security. First of all, it is the heterogeneity and multiplicity of subjects, both potentially and actually positioned to encroach on its violation of information security, as well as the diversity of subjects who have to suffer the negative consequences of all kinds of its violations. There is a problem of distinguishing the structure of communicators and recipients of information, which potentially and actually encroaches on information security. Information with various modern means of its transmission has an extraordinary speed of distribution and permeability. This, in turn, implies timeliness and adequacy of accounting and response to facts. It is obvious that different subjects can set and justify different criteria of "dangerous" and "safe", "harmful" and "beneficial". The cardinal distinction and acceptance as the content of "dangerous" in the disposition of the norm depends on socio-cultural, ideological attitudes, the state of mentality of the social group. The last circumstance is the methodologically most important condition for applying to sociological monitoring. There are a number of definitions of the concept of "monitoring" as a type of sociological research. As an example, consider the types of sociological monitoring as:

1. Monitoring (preventive, preventive) - a system of regular measurement of changes occurring in society or some of its subgroups, subject to the regular application of the same sampling principles and the same tools for data collection.

2. Socio-political monitoring - constant, systematic collection of information for the purpose of monitoring and controlling the development of some socio-political phenomenon or the process of its forecasting.

3. Case-stages - the study of individual cases of the phenomenon being studied and their intensive analysis, which includes interviewing an individual, studying documents or the incident that happened to him, analyzing the social situation in the light of the problem and formulating the main conclusions and recommendations regarding solving the problem. It is fundamentally important to distinguish this information from the information of technical systems or natural processes by methods of obtaining and interpreting social information, and this can be achieved only on the basis of a special sociological theory.

Monitoring that uses methods of collecting, processing, analyzing and using information specific to empirical sociology, such as surveys, can be called sociological. In this, the object of sociological monitoring, carried out with the help of sociological tools, can be objects of the social sphere, as well as political, economic and other phenomena. Deployment of information security monitoring is a necessary condition for ensuring information security. Monitoring significantly increases the reliability, efficiency, and effectiveness of measures taken in this field, and serves as an important means of coordinating the interests and actions of various subjects.

As part of this work, sociological monitoring was carried out on a number of main parameters and positions of the research. In this regard, one should first look at the extent to which citizens of the country are informed (know) about the existence of the Information Security Strategy of Ukraine. The author of this article conducted an empirical sociological study studying the format of citizens' understanding of the basics of the information society.

The research methodology was based on surveys as the main method of studying public opinion. The purpose of the study was to identify the main parameters of information threats in modern society, tools for managing information flows, their content and distribution channels, and directions for ensuring information security.

The issues of information security are quite clearly identified by the respondents, which made it possible to formulate a number of questions directly in terms of the social-management approach, while citizens have a relatively clear idea of the threats that are the information space, and were able, as the course and results of the research showed, to reflect and describe ( to a different degree of categorical complexity) problems of information security of modern society, namely: the nature of the meaningful parameter of incoming information threatens moral principles and social stability, the availability of information and the difficulty of limiting access to harmful or dangerous information (for example, access for children or public access to materials about violence), varying degrees of the ability to avoid receiving information (for example, the impossibility in some cases to limit the receipt of advertising or other information in the normal space of a citizen, in particular, within the limits of social networks on the Internet or in cases where the broadcast of any channel is turned on in public places).

In this regard, the following research tasks can be distinguished:

- assessment of the level of development of the institutional system of the information environment in society;
- identification of social subjects capable of the most effective social management of information security;
- the most important threats to information security, identification of key channels of dangerous information and cultural content, and selection of the most effective types of tools for countering information threats.
- analysis of the main processes of forming the information security of society;
- study of the types of main information risks, dangers and threats and their sources, their social essence and influence on the processes of formation of society's information security.

The sample consisted of 58 people. Of the total number of respondents, men made up 56%, women 44%. The age qualification was determined as follows: 10 men under 20 years, 27 men under 30 years, 12 men 30-40 years old, 9 men 40-50 years old. To the question: do you know about the existence of the Information Security Strategy of

Ukraine, the answers "yes" were received - 12 respondents, "no" - 46, which are shown in the following diagram

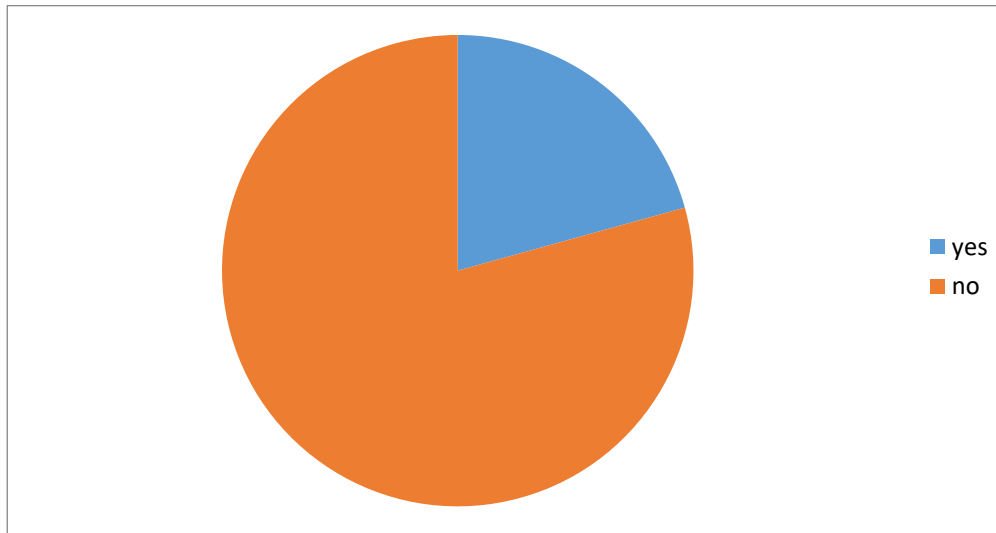


Fig. 1. Distribution of respondents' answers about knowledge about the existence of the Information Security Strategy of Ukraine.

Analyzing the obtained results, it can be concluded that the majority of Ukrainians, including young respondents, do not know about the existence of the Information Security Strategy of Ukraine, and the ratio of those who know about the Strategy and have no idea about it is approximately 1:3.8. These results can be considered typical, reflecting the general knowledge of this subject in a national format, from which we can conclude: either citizens of Ukraine do not consider information security a priority or it does not affect their vital interests, therefore they are not interested in such documents, or it is not effective enough the mechanism of popularization of such knowledge, and for all its social relevance, people have an idea about it due to inadequate information about it.

On the other hand, from the point of view, it is also remarkable that the vast majority of the respondents are students, that is, the intellectual potential of the nation, which will soon directly deal with issues of development and public administration of the country.

Interesting data were obtained as a result of the following sociological survey regarding the relevance of the current processes of forming the information security of society. To the question: which processes of forming the information security of society - technical (protection of information resources) or psychophysical (protection of social, moral-psychological, cultural and spiritual interests of the individual and society) - are currently the most relevant, the answers received from e respondents are given in the following diagram:

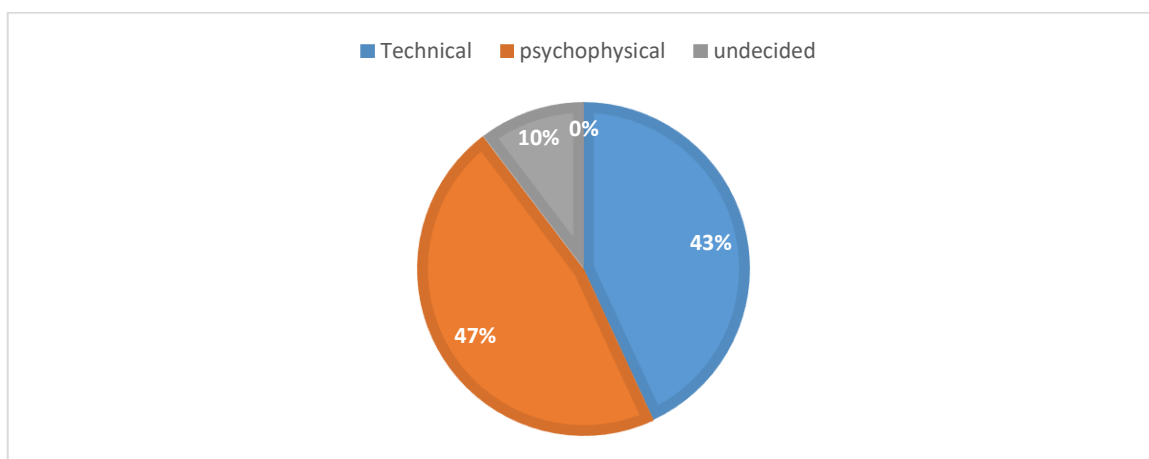


Fig. 2. Distribution of respondents' answers regarding the relevance of information security formation processes.

25 interviewees preferred technical processes of information security formation, 27 interviewees preferred psychophysical processes, 6 people were undecided. The survey data show that, in fact, the respondents consider the relevance of both to an almost equal extent (with a slight preference towards the psychophysical processes of information security formation). Thus, the social orientation of the processes of formation of information security worries and interests society, and with all the understanding of the importance of technical processes of information protection, people are quite interested in proper information protection of their social and spiritual functioning in the existing information society.

It is quite interesting to trace the attitude of the society itself, especially its young intellectual component, to the new quality (or status) that is born within it - informational. A sociological survey was conducted, investigating the format of citizens' understanding of the principles of the information society. To the question: Do you think that an information society is being formed in Ukraine, responses were received ("yes" - 43 people; "no" - 10 people; "I don't know" - 3 people), which are shown in the following diagram:

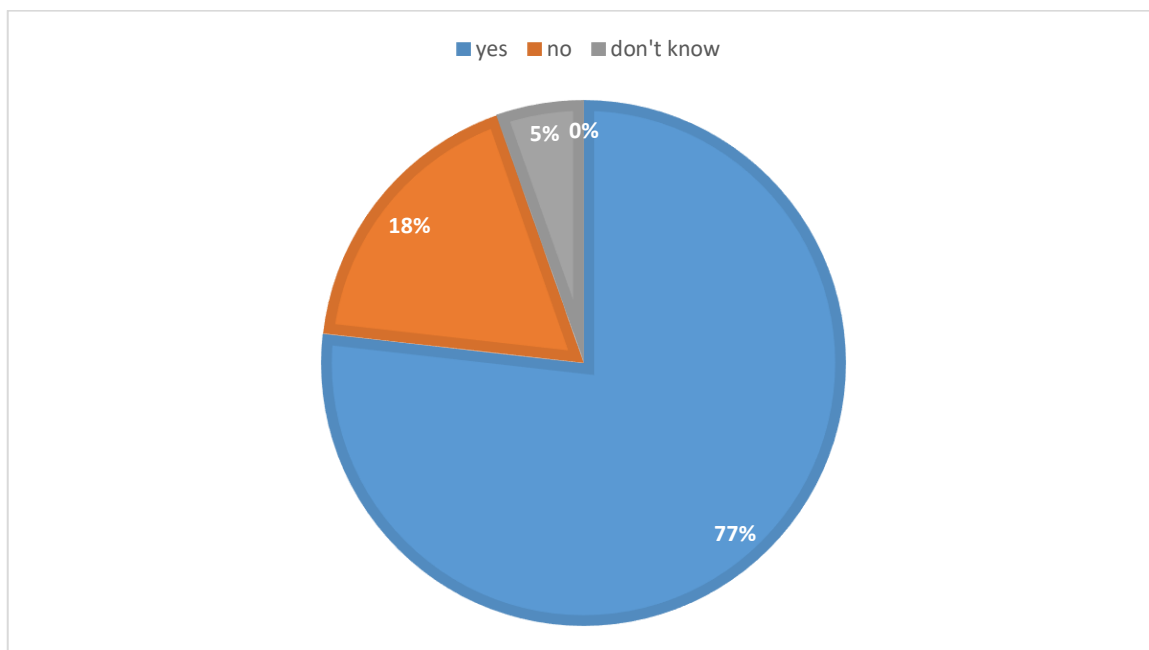


Fig. 3. Assessment of the degree of formation of the information society.

To the research question about the extent to which the emerging information society is capable of solving, on the contrary, or intensifying social problems, the respondents received answers ("to solve" - 37 people; "to worsen" - 15 people; "I don't know" - 6 people .), which are displayed in the following diagram



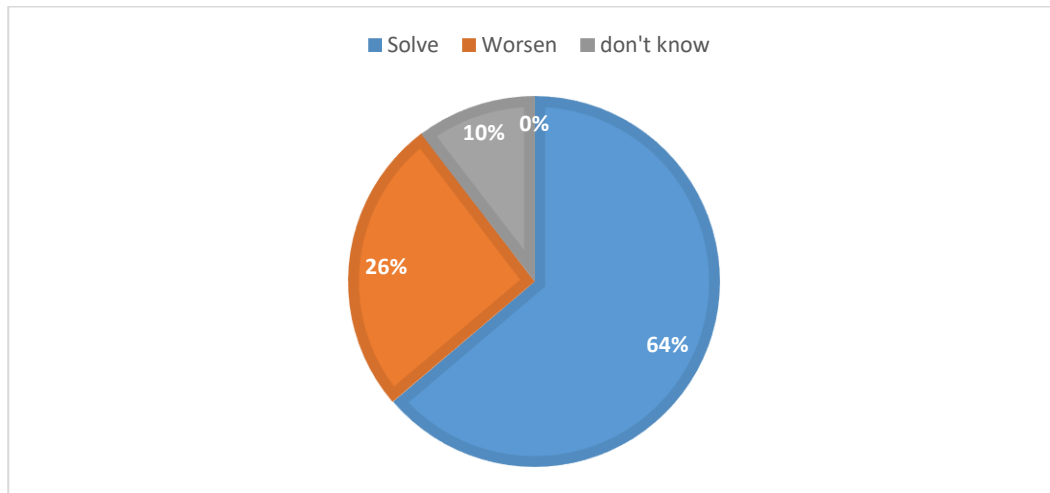


Fig. 4. Distribution of respondents' answers regarding the impact of the formation of the information society on social problems.

Considering the obtained results (and let us remind you that the main respondents of the survey are students, that is, the intellectual potential of the nation, which will soon directly deal with the issues of development and public administration of the country), it can be absolutely confidently stated that the young generation is convinced that it lives in the conditions of the formation of an information society and identifies his plans with him, believing that such a society will contribute to the solution of social problems and contribute to the development of the progress of civilization. Positive answers to these questions, according to the figures, almost double the negative and cautious ("don't know") results. Undoubtedly, the current young generation of the country has already been brought up on the basis of information and communication resources and technologies, "growing up" along with their constant improvement and cannot imagine an active life without them. To a certain extent, characterizing the obtained results, it is possible to consider that our conclusion is reinforced that the modern generations, who will come to manage the country tomorrow, are already socially and psychologically adapted to conscious life activities in the information society. Moreover, their social well-being is inseparable from the progress of such a society, and public administration of the state, as well as the solution of social problems arising in it, they identify with the

information environment. The following survey about which information threats are the most dangerous in your opinion, in total, the 9 most dangerous, according to respondents, were indicated in the following diagram:

- mass media;
- internet;
- viruses;
- rumors, gossip;
- program failures;
- hackers;
- information attacks from Russia;
- unauthorized access to the PC;
- other.

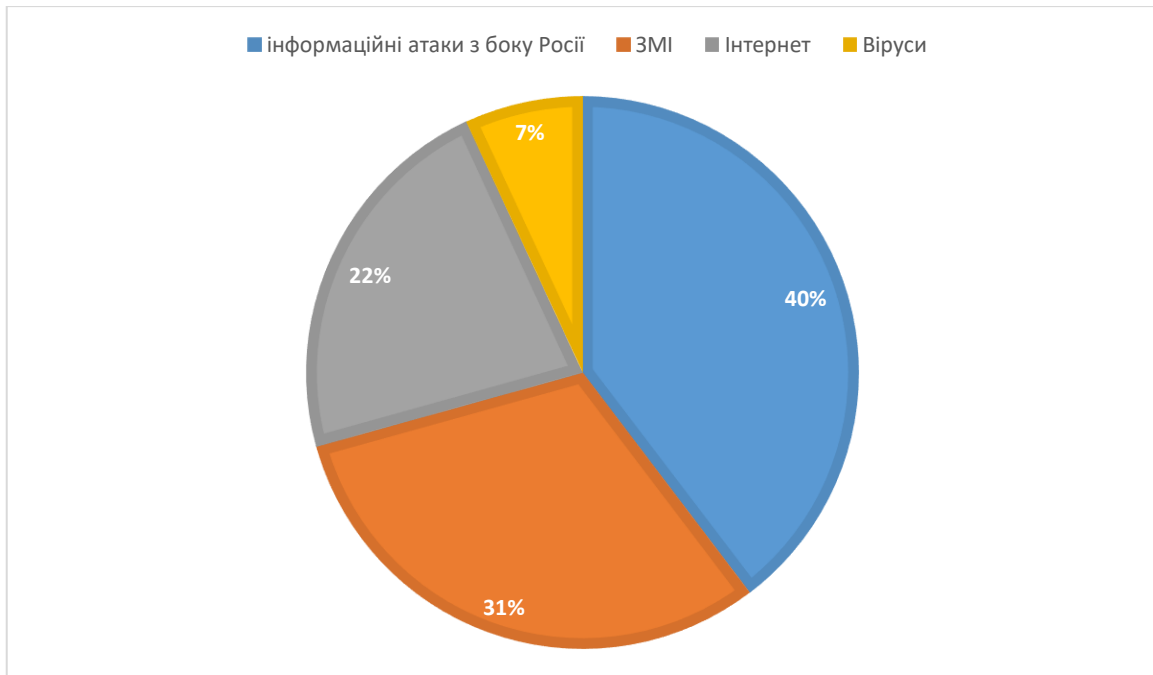


Fig. 5. Distribution of respondents' answers regarding the assessment of the degree of danger of various information threats.

The answers were distributed as follows (by descending danger of information threats): information attacks from Russia 23, mass media - 18, Internet - 13, viruses - 4. From the above survey data, one thing is obvious: the biggest concern of the respondents is information attacks by the enemies of Ukraine and the current state of mass media. In our opinion, this is due to the fact that the majority of citizens in their everyday life constantly began to face threats of a national and global nature, which pushed all other positions far back. Neither hacking nor technical problems (failures, breakdowns, disabling, unauthorized access) are of concern to the respondents. Among the reasons why mass media constitute an increased information threat, many interviewees noted the aggressiveness, vulgarity, eroticism, and primitivism of many mass media information products. According to the respondents, the Internet is a threat because pornographic sites, sites that demonstrate extremism, cruelty, torture and violence, sites that teach negative, antisocial and criminal behavior, sites that promote misanthropic ideas, etc. are extremely accessible. Other positions, according to the respondents, refer to random facts of life and do not have a permanent informational negative impact, besides, many respondents have not encountered such threats themselves and assume their presence potentially, as a phenomenon not burdened by their own empirical knowledge. At the same time, people are concerned about the social sphere, what is happening to them, in their families, in their environment, which has a destructive effect on their social life. And in this regard, people are primarily concerned about the moral and mental health of themselves, their children and loved ones, friends and co-workers, so they note as threats to social, spiritual, cultural, mental and moral well-being what encounter most often in their information field.

**Conclusions.** Thus, summing up sociological monitoring within the framework of research, we can claim that the results of sociological monitoring confirm the author's position, the expressed sociological orientation to the study of information security seems to us to be relevant and mandatory. The socio-technological format of the

processes of forming the information security of society, unlike legal, economic or technical and other formats, is today the most important and involved in the direct public management of the protection of society's interests in the information sphere.

### **References:**

1. Information Security Strategy: Approved by the Decree of the President of Ukraine of December 28, 2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
2. Google- form [https:// forms.gle/5hkbgozg4wJXcGGB7](https://forms.gle/5hkbgozg4wJXcGGB7)