



ISSN: 2350-0328

**International Journal of Advanced Research in Science,
Engineering and Technology**

Vol. 5, Issue 6 , June 2018

The selection of priority factors of the conceptual model of the state of information security

F.M.Mukhtarov

Independent employee scientific researcher, Tashkent university of information technologies of Mahomed Al-Horazmy. Tashkent.

ABSTRACT: The article presents the conceptual approaches to improve the national legislation in the field of state information security, as well as strategic planning of the state in the areas of national security.

KEYWORDS: conceptual approaches, strategy, legislation, personality, regulation.

I. INTRODUCTION

The high complexity and at the same time the vulnerability of all systems on which national, regional and world information spaces are based, as well as the fundamental dependence on their stable functioning of the state infrastructure, lead to the emergence of fundamentally new threats. These threats are primarily related to the potential use of information technology for purposes incompatible with the maintenance of international stability and security, the principles of non-use of force, non-interference in the internal Affairs of States, and respect for human rights and freedoms.

In this regard, there is a particular concern about the development, use and proliferation of new types of so-called human weapons (non-lethal weapons and technologies of war), which include information, psychotronic, economic, constant weapons and others.

Conceptual approaches include the development of normative acts, conceptual and doctrinal documents and documents of strategic planning of the state in the areas of national security, public information security, protection of state secrets, development of information society, combating crimes against information security, development of information infrastructure, the activities of the media.

The study of the problem of national information security is in demand due to the fundamental dependence of all spheres of modern society (economy, culture, science, national and international security) on the normal development and exchange of information, which is associated with the widespread introduction of new information, telecommunication and cybernetic technologies.

Information security is closely linked to ensuring state sovereignty, national security, social and economic stability and the interests of citizens. The formation of the international information security system is determined by the level of political trust between the governments of the world. As a result, there is a clear need for international dialogue on these issues, as well as the development and improvement of treaties and agreements, national and international legislation in the field of information security.

II. MAIN PART

In modern society, information security is an important component of national security. This provision is due to a number of circumstances:

- at the present stage, the implementation of the vital interests of the individual, society and the state is carried out through the processes of information, that is, these subjects see the realization of their interests through the prism of the benefits offered by the development of information relations, and want to develop in this direction;
- the information sphere has acquired the status of a system-forming and the level of economic, social, political development of society and the state largely depends on it;



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

- the specifics of the information sphere is that the negative consequences of the implementation of threats to information security are manifested in other spheres of life of the individual, society and the state and affect national security in the political, economic and other spheres;

- the analysis of existing challenges and threats in the space of States shows that in modern conditions the danger of crimes, crisis situations and other illegal actions with the use of modern information technologies increases. In such circumstances, the issues of forming an active coordinated information policy of the States, the development of a common information space, the creation of a joint capacity to counter information threats, information security, protection of information resources and communications of state, national authorities and state administration are of particular importance.

Information security is a multifaceted, complex and complex issue. Covered by a wide range of diverse problems includes the issues of information security and the institutions of the Tyne, the non-use of the Internet for military purposes, cyber security, stability and sustainability of critical infrastructure, ensure the human right to protection of personal data and the protection of intellectual property, prevent the use of counterfeit products when you use the Internet, the regulation of relations in social networks and more. Because of this, the legal norms that mediate the sphere of information security are very diverse and are contained in many legal acts in national legislation.

The specificity of information security is that in the information sphere two categories of interests of the individual, society and the state are formed: universal and special, which are a means of achieving basic universal interests (characteristic only for the information sphere. The peculiarity of the conceptual model of information security (interests – threats – measures) is that the main threats are not directed directly at the universal interests, but affect the ways of their implementation.

The description of the problem and the interpretation of the concept of "information security" are quite broad and differ in their content in different contexts. In the doctrinal political documents this concept is used in a broad sense as a state of protection of national interests in the information sphere, determined by a set of balanced interests of the individual, society and the state. In a similar context, information security is defined in the basic legislation. At the same time, the interpretation of problems related to information security may differ significantly for different categories of subjects. This fact is reflected, first of all, on the conceptual-categorical apparatus used in the field of information security.

The problem of information security is traditionally considered in the context of availability, integrity and confidentiality of information. The main focus is primarily on the processes of storage, processing and transmission of information. In everyday practice, the concept of "information security" is widely used, which characterizes a set of measures aimed at ensuring information security. The problems associated with the use of information technologies, systems and networks and, above all, in the problems of storage, processing and transmission of information under the information security in practice means the protection of information and supporting infrastructure from accidental or intentional exposure to natural or artificial nature, which can inflict unacceptable damage on subjects of information relations, including owners of information and supporting infrastructure. As a result, the problem of information security is often artificially narrowed to the technical aspects of information security, while its social and humanitarian aspects are lowered first of all. All of the above is reflected in the used conceptual apparatus, which is dominated by scientific and technical vocabulary of subordinate regulations with a variety of interpretations and weak consolidation of the terminology in the legislation. In addition, the very legal regulation acquires the features of technical, leaning towards the standardization of technological processes and moving away from the normative support of public relations.

International cooperation in the field of information security is designed to ensure the creation of mechanisms to ensure the sustainable functioning and security of information interests of the individual, society and the state. Practice urgently requires the development and improvement of cooperation in the field of combating crimes in the field of information technology.

The legal regulation provides for the solution of problems of information security, including counter-terrorism, information exchange and enforcement of legal regulations in the context of international security and development of international legislation, as well as other areas of cooperation of States in the field of information security.

The importance of this task is due to:

- the need for further development of the system of organizational and legal measures to ensure information security and the transition from the conceptual and doctrinal definition of the theoretical foundations of information security-to strategic planning directions to achieve an acceptable level of information security;

- the need to unify approaches to information protection, protection of information rights and interests and the formation of a secure information environment;



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

- the need for legal and organizational support for the implementation of national and international concepts, strategies, doctrines and plans for the development of the information society;
- the demand for maintaining political and social stability in the context of dynamic changes in the geopolitical situation and the emergence of new threats to information development, as well as the increase in information threats, implemented in the economic, political, social, scientific, technological, military and other spheres;
- the need to ensure the proper implementation of the constitutional rights of citizens and guarantees to create conditions for the free and decent development of the information space of the individual;
- the need to improve the efficiency of public authorities related to information security of the individual, society and the state.

A conceptual approach to the legal regulation of information security will strengthen and balance national information security systems. to stimulate the development of information and international information exchange.

A characteristic feature of information security legislation is that a number of institutions and norms that make up the main content of the regulatory legal support of information security are aimed at creating conditions for strict compliance with the rules governing the actual "information" relations. A number of other rules of legal support of information security develops legal mechanisms related to other branches of law, including such basic sectors as constitutional, civil, administrative and criminal law.

There is no consistency of conceptual and categorical apparatus at the national and international levels.

Significant impact on the effectiveness of information security has inconsistency of measures of legal regulation of information security with the rules governing related social relations. For example, legal measures to ensure the confidentiality of information and legal measures regulating access to information.

Common threats to information security are:

- the dominance of a number of countries in the world information space, in the production of hardware and software, and, accordingly, the backlog of a number of States in the development of information infrastructure and information security systems;
- Destructive information impact on the individual, society and the state;
- Disruption of the safe, stable functioning of critical information infrastructures;
- Unauthorized access to protected information.

In addition to common threats that are global in nature, we can consider a graded range of threats to groups of homogeneous interests of the individual, society and the state:

- threats to information security of the person;
- threats to the security of the information society;
- threats of information support of the state policy (with an exit to threats to information sovereignty of the state).

The purpose of ensuring information security is to create legal conditions for the systematic implementation of the state's balanced interests of the individual, society and the state in the framework of the state policy of the information society without outside destructive interference.

The current transformation of information and communication technologies into a fundamentally new and powerful means of destructive impact that can be directed at the objects of production and economic spheres, social infrastructure, public administration, as well as the growing threat of information terrorism require attention to critical structures and systems. These are, first of all, such complex computerized socio-technical and technical systems, the blocking or disruption of the functioning of which can potentially lead to the loss of stability of the organizational systems of state management and control, to the destruction of the system of financial circulation, disruption of the system of energy and communication and transport support of the state, global environmental and technological disasters, the loss of the defense of the state.

Taking into account the increasing danger of information crime and information terrorism on a national and international scale, as well as the increasing relevance of the problems of international information security, it seems appropriate to include the following concepts:

- information war;
- information infrastructure;
- information weapon;
- information crime;
- information space;
- information terrorism;
- strategic and critical structures;



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

- international information security;
- misuse of information resources;
- unauthorized interference in information resources.

The information and communication revolution is reflected in the transition to electronic media. This transition destroys the boundaries of the traditional information and communication process. At the same time, the scale of the impact of the information and communication environment on many aspects of society and the state is growing. The possibility of influencing public opinion has now become a significant segment of the world economy and a significant factor in the development of social and political systems, which can largely determine the lifestyle and social attitudes of a large part of society.

There are new phenomena such as social networks, blogs, individual media, etc. at the same time, today there is a convergence of traditional media, blurring the lines between the newspaper, TV and radio, and even those who are called bloggers and individual media—they all produce content of all types (text, audio, video), operate on all communication channels and use all possible means of delivery.

Currently, the problem of content reliability and ways of its verification, responsibility of those who distribute or false or erroneous content, regardless of the reasons for these actions, is growing. Therefore, it is quite logical from the standpoint of information security to impose requirements not only to improve communication technologies and technical reliability of delivery systems, but also to the quality of the content.

The concept of information security today is reflected in the documents on international information security in the wording: "Information security – the state of protection of the individual, society and the state and their interests from threats, destructive and other negative impacts in the information space" [1].

In this formulation, this basic concept covers the increasingly relevant and dangerous threats of the social and humanitarian plan, in particular, the threat of dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of the state. Such threats may be caused by both States and non-state actors, as well as by private individuals.

The main legal means of harmonization of mechanisms of legal regulation of information relations is the Association of legal regulation in the selected areas in a single legal status (individual, society and the state). Legal information status is an integrated set of opportunities for the subject to realize his rights and interests in all types of information relations [2].

Information status of the person. Provides for the implementation of the constitutional rights and freedoms of citizens in the field of information and use it:

- enforcement of intellectual property rights;
- protection from unlawful interference with privacy;
- ensuring the exercise of rights to personal data;
- ensuring the right to receive, store and disseminate complete, accurate and timely information;
- ensuring the right to information participation in public administration;
- ensuring the realization of the right to "electronic employment";
- ensuring the realization of the right to distance ("electronic") education;
- ensuring the realization of the right to e-health;
- ensuring the realization of the right to social protection.

The legal status of "safe information society". Safe information society is the information legal status of the company, which allows:

- to preserve its spiritual and moral values (traditions, cultural values);
- to develop its intellectual, spiritual and moral potential;
- to implement the activities of civil society institutions and the free dissemination of information about these activities in society;
- to resist the destructive influence of information on the public and individual consciousness, the planting of alien values and guidelines;
- to ensure the availability of publicly available information on the state of the environment, demographic and social situation, social, economic and political processes.

The status of state security (information sovereignty). Information sovereignty: the ability of the state to independently perform the functions of the state in the information sphere in order to respect the rights and freedoms of citizens, to ensure national and collective security. Aimed at:

- information support for the implementation of the state policy, which contributes to the efficiency of the functioning of state institutions;



ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 6 , June 2018

- information support of international cooperation, contributing to the expansion of presence in the world economic market and the market of intellectual products, their equal participation in world information relations and information exchange, information support of foreign policy;
- provision of innovative development, contributing to the development of modern information technology, information services industry, production of information;
- construction and safe development of information infrastructure, creating a technological basis for the management of States (in peacetime, in emergency situations and in wartime) and contributing to their interaction in the information sphere;
- ensuring the functioning of strategically and critically important information and telecommunication infrastructure (ICS), capable of ensuring the reliability and stability of their functioning;
- preservation of state secrets;
- implementation of relations in the information sphere, compliance with the laws of the information society: respect for intellectual property, rights of access to information, information exchange, the legality of information economic transactions, etc.

The legal means of coordination, harmonization of legal regulation mechanisms of information security is a complex integrating category "standard of information security". The standard of information security is a set of legal means and methods, the result of which is the proper security of the information status of the individual, society and the state.

In order to give legal measures to ensure information security, it is proposed to use the approaches of strategic planning and to consider the preparation of information security Strategy [3].

The formation of the international information security system is determined by the level of political trust between the governments of States. As a result, the need for dialogue is obvious; the development and improvement of treaties, national and international legislation in the field of information security. The solution of information security problems requires cooperation and partnership at all levels: individual, corporate, state and international.

International cooperation in the field of information security is designed to ensure the creation of mechanisms for ensuring the sustainable operation and security of the use of the global information infrastructure and its national segments, and the security of information and telecommunications technologies. Information security is closely linked to ensuring state sovereignty, national security, social and economic stability and the interests of citizens. As a result, the necessary condition is mutual understanding, equality and coordination of interests of the parties at all levels of interaction, among which there are three main ones: political-diplomatic, organizational-legal and normative-technical (technological).

III. CONCLUSION

Based on the above positions, it seems appropriate:

- consider the establishment of an organization of national entities responsible for information security;
- to consider the issue of development of standard rules of administrative procedures carried out by authorized bodies in the field of information security;
- as part of the improvement of legislation to develop a legal form of information exchange on the forms and methods of information security;
- due to the fact that, in accordance with the stated approach, information security is a complex phenomenon that integrates the results of the functioning of different – vector systems-obviously, the priority measure of improving the legislation will be the development of standard educational standards in the field of training and retraining, as well as programs for training in the field of information security. It is assumed that training in the field of information security should be modular, accordingly, it is advisable to allocate several educational institutions with the status of "master" responsible for their module.

REFERENCES

- [1] Mukhtarov F.M. "A conceptual model of information security in international relations" International Conference "Scientific research of the SCO countries: synergy and integration" April 26, 2018. Minzu University of China, Beijing, PRC p.145-151.
- [2] Mukhtarov, F. M. "Information security of state secrets in the information environment" the Herald of Tashkent state technical University №1, Tashkent, 2018, pp. 40-45.
- [3] Mukhtarov, F. M. "Conceptual approaches to the improvement of national legislation in the sphere of information security", World social science, Scientific – practical journal No. 1, p. 64-69, 2018 y.