Features ensuring information security in various spheres of the Republic of Uzbekistan

Jabbor MUKHAMMADIEV [1]

National University of Uzbekistan,Tashkent, Uzbekistan

ABSTRACT

In the international media space the issues of ensuring information security of the state is inseparably interrelated with the political, economic and legal guarantees for exercising freedom of speech and expression. The problem of ensuring the information security of any state is one of the most important aspects of its foreign policy, since it is the information sphere that is today considered to be the most important object of application of the activities of various participants in international relations. In connection with the rapid development of information technologies, threats of a new type are emerging - threats to information security on a national scale, respectively, the state must respond quickly to a changing situation and take decisive steps to organize a coherent complex information security system. The article analyzes the main approaches to providing information security of the country, formulated the goal, tasks, functions, principles of ensuring information security of the country

Ўзбекистон Республикаси турли соҳаларда ахборот хавфсизлигини таъминлаш хусусиятлари

АННОТАЦИЯ

Давлатнинг ахборот хавфсизлигини таъминлаш масалалари халқаро ахборот маконида сўз ва сўз эркинлигини амалга ошириш учун сиёсий, иқтисодий ва ҳуқуқий кафолатлар билан узвий боғлиқдир. Ҳар қандай давлатнинг ахборот хавфсизлигини таъминлаш муаммоси

[1] Candidate physical and mathematical sciences, professor National University of Uzbekistan Tashkent, Uzbekistan
Email: jabbor-1963@mail.ru

| Оммавий ахборот воситалари хавфсизлиги | унинг ташқи сиёсатининг энг муҳим жиҳатларидан биридир, чунки айнан шу ахборот соҳаси бугунги кунда халқаро муносабатларнинг турли иштирокчилари фаолиятини қўллашнинг энг муҳим объекти бўлиб туюлади. Ахборот технологияларининг жадал ривожланиши билан боғлиқ ҳолда янги типдаги таҳдидлар пайдо бўлмоқда - миллий миқёсдаги ахборот хавфсизлигига таҳдидлар, мос равишда, давлат ўзгарувчан вазиятга тезкорлик билан жавоб бериши ва изчил интеграцияланган ахборот хавфсизлиги тизимини ташкил қилиш учун қатъий чоралар кўриши керак. Мақолада мамлакатнинг ахборот хавфсизлигини таъминлашнинг асосий ёндашувлари таҳлил қилинади, мамлакатнинг ахборот хавфсизлигини таъминлашнинг мақсади, вазифалари, функциялари, тамойиллари шакллантирилади. |

Особенности обеспечения информационной безопасности в различных сферах Республики Узбекистан

Ключевые слова:
Обеспечение
Безопасность
Информационная безопасность
Средства массовой информации
Медиа безопасность

АННОТАЦИЯ

Вопросы обеспечения информационной безопасности государства неразрывно связаны с политическими, экономическими и правовыми гарантиями реализации свободы слова и самовыражения в международном информационном пространстве. Проблема обеспечения информационной безопасности любого государства является одним из наиболее важных аспектов его внешней политики, так как именно информационная сфера представляется на сегодняшний день важнейшим объектом приложения деятельности различных участников международных отношений. В связи с бурным развитием информационных технологий появляются угрозы нового типа – угрозы информационной безопасности в масштабе страны, соответственно, государство должно оперативно реагировать на изменяющуюся обстановку и предпринимать решительные шаги по организации слаженной комплексной системы информационной безопасности. В статье анализируются основные подходы к обеспечению информационной безопасности страны, сформулированы цель, задачи, функции, принципы обеспечения информационной безопасности страны.

INTRODUCTION

Today The information sphere becomes a system-forming factor of all real spheres of society activity, largely determines and effectively influences to the state of other components of the national security being at the same time its independent component, the role and importance of which is greatly increasing every year is growing steadily.

The goals and tasks of ensuring information security considered are common for various spheres of state activity. At the same time, each of these spheres has its own peculiarities of ensuring information security, which is primarily related to the specifics solution of the tasks set, the presence of weak elements inherent in each region and vulnerable links [5].

It is in this regard, each area of the state's activities has a special organization of works, the use of forms and methods of ensuring information security, taking into account specific factors affecting its state.

The most serious threats in the political sphere are: public consciousness and political orientation of various groups of the population, continuously formed under the influence of domestic and foreign media (print, radio, television, public information networks); the system of political decision-making, which essentially depends on the quality, reliability and timeliness of its information support; rights and lawful interests of citizens and public associations to the free expression of their programs, socio-political and economic orientation through the mass media, enshrined in the Constitution of the Republic of Uzbekistan [1]; the system of regular informing the population of the state administration bodies about political and socio-economic life, ecological situation through the mass media; a system of forming public opinion, including special institutions, centers and services for the identification, study and analysis of public opinion; press centers, public relations centers, media centers, Internet providers, etc.

The security of a country's information system is understood as its security from accidental or deliberate interference in the process of its functioning, from attempts to steal, modify and destroy its components. System security is achieved by ensuring the confidentiality of information, as well as the integrity and availability of system components and resources. The effectiveness of the information resources management system and their protection largely determines the general level of state security and any shortcomings in the structure and functioning of the management system for these processes lead to serious social, economic and political consequences.

When creating a system for ensuring the country's information security, the determining element is the formation of its goal. The purpose of the functioning of the information security system can be described as creating the necessary economic and socio-cultural conditions and legal and organizational mechanisms for the formation, development and ensuring the effective use of information resources in all spheres of life and work of citizens, work of society and the state.

The scientific understanding of information security as the activity of state institutions of power to protect the national interests of the Republic of Uzbekistan from threats in the information sphere occupies a significant place. The research and development of those studying political science aspects of ensuring the national and information security of the Republic of Uzbekistan includes the works of A. Aripov [3], S.M. Gofurov [4], J.U.Mukhammadiev [5,6], Saidolimov S.T.[8,9], Rasulev A.K. [10, 13], Urakov L.A. [11,12] and others.

METHODOLOGY
In this creative process, various methods of cognition were used. Among them, the dominant role is given to such general scientific methods as: dialectical (in the aspect of the relationship between "general" and "special", "abstract" and "concrete"), system-

structural and the method of abstraction, analysis and synthesis. An important role belongs to such methods as: functional, concrete historical, formal legal, comparative legal, sociological and statistical.

Among them, the dominant importance is given to scientific methods: dialectical (in the aspect of the relationship "general" and "special", "abstract" and "concrete"), system-structural, the method of abstraction, analysis and synthesis.

The integration of these methods into a single methodological position was facilitated by the contextual approach the characteristics of modern Western jurisprudence and suggesting a fundamental refusal to follow the predetermined principles and axioms until their normative and anthological significance for the growth of scientific knowledge is proved.

RESULTS AND DISCUSSION

For the democratic development of the Republic of Uzbekistan, the greatest threats are the following threats: unilateral political orientation of the mass media; propagandistic and psychological influence on the political orientation of the population of foreign and local mass media in the interests of individual political forces; imperfection of the legal mechanisms obliging state authorities to regularly and fully inform the population about their activities and the state of affairs in the sphere of their competence.

The main measures to ensure information security in the political sphere are: the development and continuous improvement of legislation, legal and organizational mechanisms regulating the relationship of all political actors in the exercise of their constitutional rights and obligations when using the media[7]; creation of a system of independent and transparent control over the activities of the media, institutions, public opinion research centers and services, as well as special communication services with the population; intensification of counter-propaganda activities and diplomatic efforts to prevent the initiation of information reasons for interference in the internal affairs of the Republic of Uzbekistan.

Objects of information security in the humanitarian sphere are people's world outlook, their values and ideals, social and personal orientations, their cultural and aesthetic positions. Evaluation of the consequences of certain information impacts in this area is very difficult and should be done taking into account the actual situation.

The sphere of a person's spiritual life is sensitive to information and propaganda influence, ideological pressure, cultural expansion, which are carried out mainly through the mass media and can be considered as information threats to the spiritual health of the population of the Republic of Uzbekistan.

Information impacts themselves are implemented in flexible, constantly changing forms, which makes it difficult to determine their impact on various components of the humanitarian sphere. This is especially true for the modern period of development of Uzbek statehood, when in essence, national priorities and state ideology are not formulated.

The prevention and neutralization of threats to information security in the sphere of humanitarian life requires, first of all, the open proclamation of official state ideology, acceptable to the majority of the population and taking into account the cultural and historical traditions of the Uzbek people. Only on the basis of this ideology can clear

criteria for assessing threats to information security, the main priority and the state policy in this sphere.

The most important is the development and implementation of civilized, democratic forms and methods of influencing the mass media in order to form and disseminate spiritual values that meet national interest, educate civil and patriotic duty and protect against hostile or unfriendly propaganda.

It's also important to have the special legal and organizational measures that hamper the commercialization of culture and ensure the preservation and development of information resources that make up the cultural and historical value.

The main bearer of spiritual values is a person constantly experiencing informational influences aimed at shaping her attitude to reality, ideals and aspirations, motivations and level of aspiration. These effects can create emotional discomfort, cause stress and disrupt the physical, social or spiritual integrity of the individual.

Ensuring the information security of the individual means realizing her rights to receive objective information and assumes her use for the purposes of free formation and development of personal and worldview qualities. As a destructive impact on the personal sphere can act: purposeful information pressure to change the world outlook, political views and moral and psychological state of people; dissemination of unreliable, distorted, incomplete information; Use of inadequate perception by people of reliable information.

A special role in influencing the consciousness bad behavior of an individual person is played by the mass media, which due to their general availability and prevalence, directly influence worldview attitudes, subjective values and preferences, regulations of actions and interaction with other people.

The organization of counteraction to threats to personal information security it is necessary to take into account the individual and personal characteristics of people, formed by previous experience, motives and interests, intellectual level, socio-demographic characteristics, social status, stereotypes, and other factors.

The choice of adequate ways of influencing (persuasion, suggestions explanation), adequate means (audio, visual, electronic, printed) depends on the completeness of accounting is a proactive information impact. One of the most important ways to counteract is a proactive information impact.

Resistance to external influences is determined by personal qualities of a person, which are largely determined by constant information influences, mainly by the mass media. They bear the main responsibility for the formation of personal and civil qualities that can withstand information threats. This is especially important at the present time, when a low level of sense of justice appears in society, people do not understand the value of information.

Information threats that cause conscious or unintentional violations of the information security of persons working in information systems and the media should be countered by explaining their rights, regulating duties and sharing responsibility, training and training staff, and in especially important cases - by selecting specialists in psychological criteria.

Among the objects of the economic sphere, the most vulnerable are the threats to information security: the system of state statistics; sources that generate information on the commercial activities of economic entities of all forms of ownership, on the consumer properties of goods and services; system of collection and processing of financial,

exchange, tax, customs information, information on foreign economic activity of the state and commercial structures[2].

The system of state statistical reporting must have sufficient security against serious and mass distortions. Particular attention should be paid to the protection of primary information sources and generalized reporting data.

Ultimately, the information in the system of state statistics should have completeness, reliability, sufficiency, comparability and regularity - the properties necessary for making rational decisions at the state, industry, enterprise levels, for conducting general economic analysis and forecasting the development of the national economy.

The normal functioning of economic objects is violated because of the lack of regulatory provisions that determine the responsibility of sources of information about commercial activities and consumer properties of goods and services for inaccuracy and concealment of information (on the results of real economic activity, on investments, etc.). On the other hand, significant economic damage can be inflicted on state and business structures due to disclosure of information containing commercial secrets.

In the systems of collection and processing of financial, tax, customs information, the greatest danger from the point of view of information security is theft and intentional distortion of information, the possibility of which is associated with deliberate or accidental violation of the technology of working with information, unauthorized access to it, due to insufficient protection measures information. The same danger exists in the bodies engaged in the formation and dissemination of information on foreign economic activity (central apparatus of departments, trade missions, customs, etc.).

A serious danger to the normal functioning of the economy as a whole is represented by increasingly sophisticated computer crimes (forgery, embezzlement, etc.), associated with the penetration of criminal elements into computer system and networks.

Along with the widespread use of standard methods and tools for the economy, the priority areas for ensuring information security are: the development and adoption of legal provisions that establish the liability of legal entities and individuals for unauthorized access and theft of information, deliberate dissemination of inauthentic information, disclosure of commercial secrets, leakage of confidential information; radical restructuring of the system of state statistical reporting aimed at increasing the reliability, completeness, comparability and security of information by introducing strict legal responsibility of primary information sources, organizing effective control over their activities and the activities of statistical information processing and analysis services, limiting its commercialization, using special organizational and software and hardware for information protection; creation and improvement of special means of protection of financial and commercial information; development of a complex of organizational and technical measures to improve the technology of information activities and information protection in economic, financial, industrial and other economic structures, taking into account the information security requirements specific to the sphere of the economy; improving the system of professional selection and training of personnel for the collection, processing, analysis and dissemination of economic information systems.

The objects of information security in the military sphere that are most vulnerable to the whole range of threats include[2]: information resources of the Ministry of Defense apparatus, the General Staff of the Armed Forces and combat arms, scientific research

institutions, containing information and data on operational and strategic plans for training and conducting combat actions, the composition and disposition of troops, the mobilization readiness, the tactical and technical characteristics of weapons and military equipment; information resources of defense enterprises, containing information and data on their scientific and technical and production potentials, volumes of supplies and stocks of strategic types of raw materials and materials, main directions for the development of weapons, military equipment, their combat capabilities and conducted in the interests of defense of fundamental and applied Research; communication and command and control systems of troops and weapons, their information support; political and moral state of troops in part, depending on the information and propaganda impact; information infrastructure, including information processing and analysis centers of the General Staff and information units of the staffs of the Armed Forces, the headquarters of associations and formations of the Armed Forces and branches of the armed forces, control posts, radio and relay links, tropospheric and satellite communications, and lines of wire communication, deployed and leased by the Ministry of Defense and other security agencies.

From external sources of threats, the following are most capable of influencing the information security of military facilities: all types of intelligence activity of foreign states; information and technical influences (methods of electronic warfare, penetration into computer networks, etc.) from potential adversaries; psychological operations of plausible adversaries, carried out by special methods and through the activities of the mass media; the activities of foreign political and economic structures directed against the interests of the Republic of Uzbekistan in the military sphere.

From internal sources of threats, the most dangerous are: violation of the established rules for the collection, processing and transmission of information in the headquarters and institutions of the Ministry of Defense, in organizations and enterprises of the defense complex; intentional acts and unintentional errors of personnel of special purpose information systems; technical equipment failures and software failures in information and telecommunication systems for special purposes; information and propaganda activities of organizations and individuals directed against the interests of the state, undermining the prestige of the armed forces and their combat readiness.

CONCLUSION

These sources of threats pose a particular danger in the conditions of aggravation of the military-political situation.

The main directions of improving information security in the military sphere are: conceptual, including the structuring of information security objectives in the defense sphere, the practical problems arising from them, the correct definition of information threats and their sources; technical, characterized by the continuous improvement of means of protecting information resources from methods and means of unauthorized access to them, the development of secure, secret communication systems and command and control of troops and weapons, increasing the reliability of special software; organizational, connected with the need to form the optimal structure and composition of the functional bodies of the information security system in the military sphere and to coordinate their effective interaction, improve methods and methods of strategic and operational concealment, intelligence and electronic warfare, methods and means of

actively opposing the information and propaganda and psychological operations of a probable enemy.

Besides that, one of the main directions for improving information security in the defense sphere is to increase the efficiency of protecting production technologies and tactical-technical characteristics of weapons and military equipment.

Today, the information sector acts as the most vulnerable component of the overall national security system. The normal life of society has become entirely determined by the level of development, the quality of functioning and the security of the information environment. Threats to information security are objective in nature, due to the current political process and are closely linked to changes in the information sphere based on the development of information technologies. The revealed regularity is expressed in the expansion of the scale of threats to information security by foreign states through information and information-psychological influences. An increase and expansion of the spectrum of information security threats increases the role of the state in the implementation of a strong information policy in practice, the close attention of society to the educational sphere that directly affects information technology today, and the improvement of the legal regulation of the activities of citizens and states in the information sphere.

REFERENCES:

1.The Constitution of the Republic of Uzbekistan. 2018, p.72.

2.Alimov R.M., Mukhammadiev J.U. Features of ensuring information security in various spheres of life activity of the state and society. Scientific and practical conference "Problems and solutions in the use of information and communication technologies in public administration and the education system." - T.: Tashkent State University of Law, 2017. p.p. 278-282.

3.Aripov A. The media sphere of Uzbekistan: the ways of democratization of the media. Journal of the «Фуқаролик жамияти.Гражданское общество. Civil Society». - T. №6, 2005. p.p. 56-59.

4.Gofurov S.M. Methodological aspects of studying the problems of national security. Oriental studies. –T.: №2, 2005. p.p. 93-96

5.Mukhammadiev J.U. The purpose, structure, principles, methods and tasks of legal support of information security. - T.: Tashkent State University of Law, 2009. p.p. 80-82.

6.Mukhammadiev J.U. Structure of legal regulation of relations in the field of information security. Journal of the "State and Law". –T.: №6,2006. p.p.54-56.

7.Mukhammadiev J.U. Information security and its support: legislative, administrative, procedural and software-technical levels. Journal of the "Legal fact" №23, 2018 RUSSIA (Kemerovo). Pp. 76-80

8.Saidolimov S.T. Features of some conceptual approaches to security. International relations. –T.: No. 3, 2005. p.p. 16-23.

9.Saidolimov S.T. Some aspects of security research. Oriental studies. –T., №2, 2005. p.p.96–100.

10.Rasulev A.K. Prospects of development of legal protection of information technologies in Uzbekistan. Under the protection of the law, 2002. №6 (78) – p.p. 21-23

11.Urakov L.A. New information technologies in the tasks of ensuring national security of the Republic of Uzbekistan (natural and technogenic aspects): Monograph. -T .: "AL-FABA SERVIS", 2003. pp. 212.

12.Urakov L.A. Information Security: New Threats to the World Community.-T .: VCU MCV, 2001. pp. 164.

13. Rasulev A.K. Crimes in the Field of Information Technology and Security: Determinants and Warnings. Vol. 1 No. 1 (2020): Society and innovations. – P. 200-209. (https://inscience.uz/index.php/socinov/article/view/29 // https://doi.org/10.47689/10.47689/2181-1415-vol1-iss1-pp200-209)