REGULATORY LEGISLATION OF TECHNICAL PROTECTION OF INFORMATION IN EMERGENCIES

Svitlana Usyk

Ph.D. Student, Institute of Public Administration and Research in Civil Protection, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7219-3727

Abstract. The basis of state regulation of public relations in the sphere of technical protection of information is the Constitution of Ukraine. The special legislation regulating this branch includes the Laws of Ukraine: "On Information", "On State Secrets", "On Protection of Information in Automated Systems", "On the National System of Confidential Communication", "On the Concept of the National Informatization Program", "On scientific and technical information" and others. Including in the sphere of law enforcement - those that determine the competence and functions of certain state authorities: the Security Service of Ukraine, the Ministry of Internal Affairs, etc.

Some requirements for the technical protection of certain types of information are contained in the legislation of Ukraine on operational and investigative activities, on the organizational and legal framework for combating organized crime.

The state policy of Ukraine in the sphere of protection of information from its leakage through technical channels is reflected in the system of bylaws of public authorities, issued by the latter in accordance with their competence, functions, rights and responsibilities. This system consists of Decrees and Orders of the President of Ukraine, regulations of the Cabinet of Ministers of Ukraine, regulations of the Security Service of Ukraine, other ministries and departments.

Keywords: *technical protection, automated systems, information security, emergency, protection of human and civil rights.*

Introduction

Regarding standardization in the sphere of technical protection of information, it should be noted that in addition to state standards of Ukraine. Also technical protection of information is also regulated by regulations of the technical protection of information, which do not belong to normative documents on standardization, but are mandatory all central and local bodies of state executive power, local self-government bodies, military units of all military formations created in accordance with the legislation, enterprises, institutions and organizations, regardless of ownership, whose activities are related to technical protection of information. And finally, the provision on technical protection, which, unfortunately, was not reflected in the acts of the highest level. Settled for individual organizations, institutions and state bodies by relevant departmental orders, directives and instructions that regulate the activities of units of technical protection of information, as well as help to solve certain specific tasks of technical protection of information. We refer them to acts of other bodies issued by them within the given competence.

However, the state of legal regulation of both technical and general protection of information currently suffers from the lack of solutions to a number of problematic issues, which, unfortunately, still do not have the relevant regulations.

The aim of the article is to study state of regulatory legislation of technical protection of information in emergencies.

Literature review. Prokofiev M., Khoroshko V. during the study of the problem technical protection of information make evident, that laws and subordinate acts make up the top echelon of documents regulating the legal relationship in Industries of technical protection of information(Prokofiev, Khoroshko, 2015, pp. 9-14). It can only conceptually identify some approaches and features of technical protection of information.

The main content of labors on technical protection of information and evaluation of their effectiveness contained in a special regulatory documentation. The presence of a comprehensive, functionally complete documentation system regulating all stages conducting measures of technical protection of information, as well as the entire life cycle of it (development, manufacturing, testing, operation, repair, storage and utilization) is a rather important system-forming factor that impact on efficiency of the entire technical protection of information system in the state. Therefore, the creation of a scientifically substantiated system of normative documents is a fairly relevant task.

Although there are currently some number of normative documents responsible for individual issues and give ability to solve some tasks in separate directions of technical protection of information. The main solution of this problem is seen in the establishment of a system of standards and regulatory documents in branches of technical protection of information.

Gerashchenko Y. in the study observes, that under conditions of rapid formation and development of information society in Ukraine and global information process, intensification of information and communication technologies in all spheres of life, and there is a threat of security (Gerashchenko, 2019, p. 140).

As a result of the absence of an effective system of information security in the national information process, there is a large number of negative phenomena that create real and hidden threats.

However, the information component becomes one of the most important elements of national security. Information space, resources, infrastructure and information technologies significantly affect the level of socio-economic, scientific, technical and cultural development. This is the level of development and safety of the information process, which is systematic factors in all areas of national security, which actively affect the state of economic, political, defense and other components of national security.

Frolov O. in research asserts that the normative legal acts in Ukraine and normative documents are not enough to resolve problems of protection of information as a whole and technical protection in particular (Frolov, 2008, p.7).

There is a problem of personal data protection individuals and the protection of open information aimed at realizing the legitimate rights and interests of the person, society and state. In recent years, the laws of Ukraine regarding the protection of information in information and telecommunication systems, licensing, state control of economic activity, confirmation of conformity, me provision of activities related to the measurement of physical quantities, require conducting certain measures to bring the system of information in accordance with the requirements of these laws. The results of state control over the state of technical protection of information in Ukraine are evidenced by not complete compliance with state bodies with the requirements of applicable normative legal acts and normative documents that due to the lagging of actual funding for providing information protection from real needs for the realization of appropriate measures.

Researcher Tverdokhlib O. in the study notes that the state policy in the sphere of informatization is aimed at creating conditions to effectively meet the information needs of the person, society and states based on access to information and use information systems and technologies (Tverdokhlib, 2012 p. 8,9). Among the main directions of state policy in this area it is necessary to name the formation, development and protection of state information systems and information and telecommunication networks.

Their compatibility and interaction in a single information space, creation and development of national and municipal information systems for information support of citizens, organizations, state authorities and local self-government, including based on the introduction of electronic document management systems, which also requires general technical protection of information.

Research methodology. To achieve the aim**,** general scientific and theoretical methods were used, in particular: empirical, synthesis, classification. Research methods for existing connections are used as common methods of analyzing the level of information security.

These methods reveal the causal links between threats and dangers; the search for the causes that have become the source and caused the actualization of certain risk factors, as well as measures are being developed to neutralize them. Among these methods of

causation are the following: the method of similarity, the method of discrepancy, the method of combining similarity and discrepancy, the method of accompanying changes, the method of residues.

Research results. From the analysis of the legal framework for information protection in automated systems, it influences that in modern conditions the importance of information protection is given to the creation of a system of technical protection of information. In the public law of Ukraine, the system of technical protection means a set of entities united by the goals and objectives of information protection by engineering and technical measures, regulatory and material and technical base.

The problem is especially determined in Ukraine by the following factors:

- normative uncertainty of concepts and categories, in particular at the level of legal acts (documents);
- imperfection of legal regulation in the information sphere, in particular in the sphere of protection of secrets (except state), confidential information and open information important for the person, society and the state and technical protection of information in general;
- insufficiency of normative legal acts and normative documents on the issues of conducting research, development and production of means of ensuring technical protection of information;
- incomplete creation of a system of certification of technical information security means;
- imperfection of the certification system for compliance with the requirements of the technical protection of information of objects whose work is related to information subject to technical protection;
- insufficient harmonization of normative legal acts and normative documents on technical protection of information in force in Ukraine with the relevant international treaties of Ukraine.
- unclear regulation of technical protection of information in ministries and departments of Ukraine.

It is noted that the volume, speed and quality of information processing largely depends on the effectiveness of management decisions, the importance of management methods using information technology by social and economic processes is growing, and most importantly - the ability to identify scientific, technical and environmental problems, monitor their development with further forecasting of consequences, which directly depends on the effectiveness of information infrastructure and its protection.

At the present stage, the main real and potential threats to Ukraine's information security in the environmental sphere are concealment, untimely provision of information or provision of inaccurate information to the population about environmental emergencies or man-made and natural disasters. Insufficient reliability or general insecurity of information and telecommunication systems that are responsible for the:

- collection, processing and transmission of information in emergency situations;
- low level of informatization of public authorities, which makes it impossible to carry out operational control and analysis of the condition of potentially dangerous objects and territories, early forecasting and response to emergencies.

That is, the security of the country's information infrastructure in case of accidents, catastrophes and natural disasters is of special importance for the full functioning of state facilities.

In our opinion, ensuring information security in emergencies is ensuring the security of information systems that facilitate decision-making on operational actions related to the development of such situations and the course of elimination of their consequences, as well as ensuring the security of information collection and processing systems in emergencies.

Concealment, delay of receipt, distortion and destruction of operational information, unauthorized access to it by individuals or groups of persons can lead to human casualties and to various difficulties in dealing with the consequences of an emergency related to the information impact in extreme conditions to:

- set in motion large masses of people experiencing mental stress;
- the rapid emergence and spread among them of panic and riots based on rumors, false or unreliable information.

It should be noted that negative impacts on information security facilities can lead to serious damage to vital interests and cause significant socio-economic losses to the state,

society, the reputation of the SES of Ukraine and its structures, and individual citizens (Barrel, pp. 147-148). Information security activities, including in emergencies, are manifested in the form of social regulation, including legal, as well as political activities and organizational measures to combat threats to national interests in the information sphere.

Certain provisions of normative legal acts of the legislation of Ukraine regulating relations in the sphere of human and civil rights and freedoms are internally contradictory and, in some cases, do not comply with the norms of international law. Excessive declarativness of some legal norms leads to the fact that their violation does not always entail the occurrence of appropriate liability, which significantly reduces the effectiveness of legal regulation of these relations by law and creates preconditions for victims to apply to international courts.

A number of the most serious shortcomings of the legal provision for the protection of human and civil rights and freedoms in the information sphere include:

- imperfect definition of mechanisms to ensure access to open information of public authorities and local governments, which creates conditions for violation of human and civil rights and freedoms, including the right to information about the state of the environment, facts and circumstances that threaten life and health;
- lack of established rules of liability for restriction or violation of the right to access public information;
- lack of state regulation of the dissemination of information intended for an unlimited number of consumers in open information and telecommunication networks.

Among the main shortcomings of the legal security of information and telecommunications systems and communication networks, Ukrainian information resources are:

- disproportions in the development of the general component of state legislation, the presence of contradictions between them, as well as the lack of legal framework for the coordination of legislative activities of Ukraine and its subjects;
- insufficient normative-legal state regulation of relations in the sphere of development of technical protection of information while ensuring information security;
- insufficient effectiveness of legal mechanisms for establishing liability for offenses in the sphere of information security.

Discussion of research results. At the present stage, the main real and potential threats to Ukraine's information security in the environmental sphere are concealment, untimely provision of information or provision of inaccurate information to the population about environmental emergencies or emergencies of man-made and natural nature; and insufficient reliability of information and telecommunication systems for collecting, processing and transmitting information in emergency situations.

That is, the security of the country's information infrastructure in case of accidents, catastrophes and natural disasters is of special importance for the normal functioning of state facilities.

In our opinion, ensuring information security in emergency situations is ensuring the security of information systems that facilitate decision-making on operational actions related to the development of such situations and the course of elimination of their consequences, as well as ensuring the security of information collection and processing systems. emergencies.

Concealment, delay of receipt, distortion and destruction of operational information, unauthorized access to it by individuals or groups of persons can lead to human casualties and to various difficulties in dealing with the consequences of an emergency situation related to the information impact in extreme conditions to:

- set in motion large masses of people experiencing mental stress;
- the rapid emergence and spread among them of panic and riots based on rumors, false or unreliable information.

It should be noted that negative impacts on information security facilities can lead to serious damage to vital interests and cause significant socio-economic losses to the state, society, SES of Ukraine and its structures, and individual citizens.

Conclusions

The problem of state regulation in the sphere of information security in emergencies is complex and includes the regulation of legislation.

Issues of ensuring the security of the information system of prevention and elimination of the consequences of emergencies, as well as the system of collection, processing, exchange and issuance of information in the sphere of protection of the population and territories from emergencies of natural and man-made nature, are not legally reflected in regulations State Emergency Service of Ukraine. In this regard, the paper formulates proposals for improving the current legislation in the sphere of information security in the protection of the population and territories from emergencies of natural and man-made nature.

State regulation of technical protection of information and information security in emergency situations is an independent component of the direction regulatory and legal support of information security in general, carried out in the framework of the state policy in the sphere of information security. Norms governing the legal provision of information security in emergencies form a comprehensive legal institution and regulate public relations to protect national interests in the information sphere (vital interests of the individual, society and the state on a balanced basis) from threats in emergencies.

Analysis of the main regulations governing the activities of units of the SES of Ukraine, allows us to conclude that the degree of participation of the SES in civil defense, emergencies and liquidation of violence. The number of natural disasters in the legal provision of information security of Ukraine in emergency situations is quite high. The SES of Ukraine participates in the performance of coordinating functions in the sphere of information security in emergency situations. Correct determination of the competence of this body of executive power in the sphere of counteracting threats to national interests in the information sphere and organization of its interaction with the President of Ukraine, the Cabinet of Ministers and other services of our state.

References

1. Barrel O. (2011). Estimation of the amount of useful information by public administration bodies in emergency situations: Economy and state. (3) pp. 147–148.
2. Doctrine of Information Security of Ukraine (2016). Decree of the President of Ukraine of 25.02.2017 № 47/2017 // Database "Legislation of Ukraine". Verkhovna Rada of Ukraine. [Electronic resource]. Available at: https://zakon.rada.gov.ua/laws/show/47/2017
3. Frolov O. (2008). Legal, normative and metrological support of the information protection system in Ukraine: (16), p. 7. [Electronic resource]. Available at: *https://core.ac.uk/download/pdf/47227963.pdf*
4. Gerashchenko Y. (2019). Legal, normative and metrological support of the information protection system in Ukraine: scientific and technical collection. (16). p. 140.
5. Prokofiev M., Khoroshko V. (2015). Legal, normative and metrological support of the information protection system in Ukraine: scientific and technical collection. (30). p. 9-14.
6. Tverdokhlib O. (2012). Legal regulation in the sphere of information public-administrative resources of Ukraine. 2012. pp. 8-9. [Electronic resource]. Available at: http://www.dridu.dp.ua/vidavnictvo/2009/2009-02(2)/Tverdokhlib.pdf