DOI: 10.18372/2307-9061.59.15600
UDC 342.924(045)

Viktor Moroz,
Senior Lecturer
ORCID ID: https://orcid.org/0000-0002-7070-0104

FEATURES OF INFORMATION SECURITY IN MARTIAL LAW

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: victor.moroz@npp.nau.edu.ua

Purpose: *the article is devoted to the analyze of the features of information security in martial law.* ***Research methods:*** *comparative analysis of individual regulations and the case law of Ukraine regulatory framework and case law in the application of the information security in martial law.* ***Results:*** *normative regulation of the formation of a single information space in Ukraine should contribute to the harmonious development of information resources, information services and the information product in the country. Improving the effectiveness of the subjects under investigation countering threats to information security.* ***Discussion:*** *the analysis of the legal the features of information security in martial law is carried out.*

Keywords: *features; information security; martial law; military aggression; wide range of domestic researches.*

Formulation of the problem. The significance of the topic is due to the problematic nature of the functioning of political power in the current conditions, the need to establish a mechanism for the separation of state power.

The effectiveness of the exercise of power in any state, including Ukraine, depends to a large extent on its information support. Without information, it is impossible to imagine a positively functioning political structure, the development of mass political consciousness, the interaction of the subject and the object of politics. In the process of information and communication influence in the consciousness of the people, the image of state power, its political institutions and leaders is formed, and the governing functions of the state are carried out with the greatest potential and the lowest energy costs only when the information communication system between the state, civil society and the individual is well developed. In modern society, information technology is one of the most important drivers of social change. In Ukrainian science, there is growing interest in studying the prospects for the formation of the information society in Ukraine. A wide range of problematic phenomena is associated with the information security of the individual, society, and the state.

Russian military aggression aimed at the forcible unlawful rejection of Crimean autonomy and Sevastopol from Ukraine and their accession to the Russian Federation as a subject of the Russian Federation, which was carried out during March 2014, Russia's military invasion of Donbass, aircraft crash "Boeing-777" Malaysian Airlines and many other events of this kind that occurred in our country revealed the obvious failure of the previous structure of national security, created to neutralize the threats characteristic of the cold war.

New challenges and threats have emerged that put the world on the brink of catastrophe: international terrorism; organized crime; illicit trafficking in drugs and weapons; racial intolerance; religious bigotry; political extremism; aggressive separatism. There are threats in such an important area of international cooperation, the integration of the entire world community, such as information. Information is directly related to political processes in the modern world. The results of the development of information technologies make it possible to hope for the creation of a dynamic world information model. Over the past years, the intensity of information consumption in all spheres of human life and society has increased incredibly - social, scientific, technical, technological, statistical, economic, etc. The processes of collecting, accumulating, processing and disseminating information become a prerequisite for existing structures of political and other governance, the implementation of effective political influences, and the solution of large-scale economic problems.

However, information is not only a force. Unfortunately, it has a destabilizing potential for society if it`s almost unlimited possibilities of influence over people and society are used for the benefit of coalition communities, individual states, political groups or individuals. The experience of the recent history of the world has determined the obvious: information can become a source of political and social threats, which is due to the relevance of information security research, especially in martial law.

The purpose of this article is to study the key features of information security during martial law in order to improve the legislative mechanisms governing the use of information and the introduction of effective practices for the application of such norms in modern realities.

The research was carried out using the general scientific dialectical method, as well as such special methods of scientific knowledge as the method of materialist dialectics, which is used to clarify the essence of the relations, patterns and features of their functioning and comparative legal method - comparative analysis of individual regulations and the case law of Ukraine regulatory framework and case law in the application of the information security in martial law.

Analysis of recent research and publications. Information security issues, including martial law, is the subject of research by a wide range of domestic and foreign researchers. Thus, the issue of information security is reflected in the works of such domestic scientists as V. Bogush, V. Bogdanovich, M. Bychenko, V. Gorbulin, R. Grischuk, T. Dziuba, D. Dubov, I. Zamarueva, Ya. Zharkov, S. Zhuk, D. Lande, V. Lipkan, A. Litvinenko, V. Ostroukhov, M. Ozhevan, V. Panchenko, V. Petrik, A. Manoilo, A. Panarin, G. Pevtsov, G. Pocheptsov, M. Pryasnyuk, A. Ros, A. Semenchenko, V. Snitsarenko, V. Telelim, V. Tolubko. and others. Significant contribution to the study of the issues of information security was made by such foreign scientists, like M.M. Kucheryavy, I.V. Bernatsky, M.K. Gorshkov and others. However, despite the large number of publications related to this topic, there are still many controversial issues, due primarily to legal practice, as well as due to the dynamic development of the field of information security in the modern realities of martial law.

Main material. The analysis of recent studies and publications revealed a discrepancy between the capabilities of the current system of information security measures, which is based on outdated approaches with an inefficient organization of operation, and the modern system of information security measures, which would ensure the full implementation of all assigned and promising tasks. At the same time, it was established that the unresolved part of the general problem of ensuring the information security of the state in the military sphere remains the problem of creating holistic scientifically sound methodological foundations for the construction and functioning of an information security system in the military security system.

Today, the state of information security is characterized by an increase in the use by individual states and international organizations of information technologies for military and political purposes, in particular for the implementation of actions contrary to international law aimed at undermining sovereignty, political and social stability, territorial integrity and posing a threat to peace, global and regional security.

This state of information security requires further study, which leads to the relevance of the study.

At the beginning of the XXI century, state activity in the legal sector is significant and has changed dynamically, but the changes that have occurred so far have not received their systemic, comprehensive scientific and theoretical analysis, in information security. This is particularly true of safeguards issues and protecting the rights and freedoms of citizens, maintaining the information security of the person who becomes an independent subject of state policy.

The military security of the state has been and continues to be one of the priority areas for ensuring the sovereignty of Ukraine, its territorial integrity and the inviolability of its borders. Changing the nature of military threats at the present stage of the development of military art and forms and methods of conducting armed struggle, the hybrid nature of enemy actions puts forward new requirements for the system of ensuring the military security of the state in all areas, including the field of information security.

Social stability and national security are defined by the content of the information space, in which both individuals, social groups, organizations and states, political groups and forces carry out their activities. So, the famous sociologist M.K. Gorshkov writes that modern ways of impact on mass consciousness of people are old as the world, and it is only necessary to create the myth and to force to believe in it, but in modern conditions of information society it became much easier, simpler to make it, and as a result information and network wars became real threat to security of the state [1].

The concept of "peaceful and martial law" intertwined in virtual space, giving rise to the terrible phenomenon of "information war," which is able to draw millions of people into the area of military information actions in a short period of time. Distances, borders, temporary and other obstacles to the world of real in virtual space mean nothing, therefore, information weapons have become a powerful weapon of the XXI century, under the aim of which there is both a separate individual and humanity as a whole.

The concept of peace has become precarious, unsustainable and conceptually blurred, as wars, apart from actual hostilities, which unfortunately still take place in society, have also moved to a virtual space, where "military" actions and events also unfold, battles for domination of the masses and their consciousness take place. The main weapon in this war is information and communication technologies. The concept of war has expanded its conceptual framework since the formation of the global information system, but the spread of virtual wars and the Internet has the most real consequences and not only in changes at the level of mass consciousness and behavior, but also in the military-political strategies of states.

The possibilities of the unlimited movement of information are more often used to achieve geopolitical, military-political, as well as terrorist, extremist, criminal and other illegal goals at the expense of international security and strategic stability.

One of the main negative factors affecting the state of information security is the strengthening of the capabilities of information and technical influence on the information infrastructure for military purposes. At the same time, the activities of organizations conducting exploration regarding the work of scientific organizations and enterprises of the state, in particular the military-industrial complex, are intensifying.

The use by the special services of the aggressor states of means of information and psychological influence aimed at destabilizing the domestic political and social situation in various regions of the world and leading to the undermining of sovereignty and violation of the territorial integrity of states is spreading. Religious, ethnic, human rights and other organizations, as well as certain groups of citizens, are drawn into this activity, because of this, the possibilities of information technology are widely used.

There is a tendency to increase the volume of materials in foreign media containing a negative, false (subversive) assessment of state policy and the leadership of the state against which the aggression is carried out.

Information influence on the population is growing, primarily on young people, to erode traditional spiritual and moral values.

Various terrorist and extremist organizations widely use mechanisms of information influence on individual, group and public consciousness to increase ethnic and social tensions, incite ethnic and religious hatred or enmity, and promote extremist ideology.

Computer crime is on the rise, especially in the financial and credit sphere, and the number of crimes related to the violation of constitutional rights and freedoms of a person and a citizen is increasing, in particular with regard to privacy, personal and family secrets, in the processing of personal data using information technologies. In addition, the methods and means of committing such crimes are becoming more sophisticated.

The scientific community, now, identifies three conceptual approaches to interpreting information security: 1) static (security as a state of security of the information environment/information, guarantee system, etc.), 2) operational (security as the process of ensuring it, the ability of the state to effectively protect national interests and values); 3) complex (security as state and process).

In my opinion, the most complete is a complex approach to determining information security, according to which information security is on the one hand a state in which, in the face of real and potential threats, self-preservation, sustainable and progressive development information sphere, in particular security of information infrastructure, information space, information resources, information processes and their actors, as well as achievements of relevant national objectives and realization of national interests in the field of information, and on the other hand, a continuous process of activities of the competent authorities aimed at prevention, counteracting threats in the information sphere, application active measures of information impact, as well as a set of conditions as such activities that are implemented and able to be monitored for a long time.

Ensuring information security of Ukraine is the defining direction of state policy, on which it will depend existence of the state, its national security, socio-economic development and an appropriate place in the world community.

Main objectives of state policy of information security in Ukraine are: a) information security sovereignty of the state in the current conditions of globalization and Internationalization processes in the information sphere; b) provision of information sufficiency for decision-making by state bodies, enterprises and citizens; c) realization of constitutional rights and freedoms of citizens, society and state on information.

The legislative definition of the concept of "information" is contained in the Law of Ukraine "On Information", according to Art. 1 of which: "Information is any information and/or data that can be stored on tangible media or reflected in electronic form" [2]. A similar definition is contained in part 1 of Art. 200 of the Civil Code of Ukraine.

In the context of our study, it is necessary to draw attention to the content of the category "security", which in human life acts as a reference point around which the values of human existence are grouped. This concept is multifaceted, on this occasion there are many opinions in science. Literally, security means no danger. The need for safety is among the basic motivational mechanisms in human life, and in this regard man is little different from any of the other living beings. Moreover, security is an undeniable and universal value, as it is recognized by all people regardless of their race, nationality or social affiliation.

The importance of protecting information security is stated in the Constitution of Ukraine: "Protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the issue of the entire Ukrainian people" (art. 17) [3].

The legislative definition of information security is recorded in the Law of Ukraine "On Basic Principles for the Development of the Information Society in Ukraine for 2007-2015": "Information security is a state of protection of vital interests of a person, society and the state, in which damage is prevented through: insufficiency, untimeness and disadvantage of the information used; negative information impact; the negative impact of information technology; unauthorized distribution, use and violation of the integrity, confidentiality and accessibility of information" (p. 13 of the Law) [4].

Information security is a complex, systemic, multi-level phenomenon, the state and prospects of which are directly influenced by external and internal factors, the most important of which are: 1) the political situation in the world; 2) presence of potential external and internal threats; 3) state and level of information and communication development of the country; 4) the domestic political situation in the state. At the same time, information security is a complex, dynamic, holistic social system, the components of which are the security subsystems of the individual, the state and the society. It is the interdependent, systemic information unity of the latter that constitutes qualitative certainty designed to protect the vital interests of man, society and the state, to ensure their competitive, progressive development [5, p. 154-155].

Experts call an important component of hybrid warfare - an invasion of the information and communication space of a certain country in order to suppress resistance and form a world political standard consistent with the interests of the aggressor. To do this, a wide variety of tools are used to manipulate public opinion: interference in the functioning of information and telecommunication systems and networks; the development of cybercrime; influence on mass communication and manipulation of public opinion [6, p. 18].

As M. Dmitrenko rightly observes: "The nature and peculiarities of the Russian-Ukrainian war indicate that its goal is to change the self-identification of the population and turn the eastern region of our state into a "gray zone", which will leave the Russian Federation levers of its influence due to the constant threat of spreading instability throughout Ukraine. This is a war not for territories, but for the worldview, thoughts and souls of people. And since control over the information infrastructure gives grounds for the formation of public opinion, which always first turns out to be in certain convictions, and only then in specific actions, then in the conditions of competition, control over the information sphere turns into one of the main resources of power" [7, from 40-41].

The provision of information security is characterized by special the way of regulatory influence on public relations, which is noted positive consequences. The specificity of the use of individual administrative legal means in the regulatory process is largely due to a feature of a legal construct that determines the intensity of an expression in each of the stimulating, compensatory, guaranteeing foundations. Legal means, designed to achieve the goal, perform two main functions: compensatory and stimulating. They have clear goals and objectives administrative and legal regulation in the field of information security, legal nature and social purpose. In addition to these, they perform, like any other legal means, security, educational, communicative, motivational, value-oriented and social control functions.

Almost everything is used to ensure information security types of administrative coercion measures (prevention, termination, recovery) and measures to secure administrative proceedings offences.

Take into account the public nature of the purpose of the state in respect of ensuring information security arising from peremptory norms established legal regimes, and not always balance of public and the private side of information legal relations is related to tasks states to achieve this objective.

It is advisable to take into account the significance of security tasks information security: both general prevention and incentives support of information activity subjects - owners of critical facilities information infrastructure. Meeting these challenges will help improving the effectiveness of the subjects under investigation countering threats to information security.

The specifics of ensuring national information security are reflected in the Laws of Ukraine "On National Security of Ukraine" [8], "On the Concept of a National Informatization Program" [9], "On basic principles of information society development in Ukraine for 2007-2015 years" [10], as well as in the National Security Strategy of Ukraine approved by the presidential decree [11], in connection with the implementation of the Strategy, the National Security and Defense Council of Ukraine decided to create a special new body as a working body - the National Coordinating Center for Cybersecurity. The creation of such a center is justified, since a significant number of state bodies and institutions have the authority to ensure information security (the National Council of Ukraine for Television and Radio Broadcasting, the State Committee for Television and Radio Broadcasting of Ukraine, the Security Service of Ukraine, the Foreign Intelligence Service of Ukraine, the Ministry of Defense of Ukraine, the Ministry of Foreign Affairs of Ukraine, the Ministry of Justice of Ukraine, etc.).

The national security strategy of Ukraine with current threats to the national security of Ukraine in the information sphere determines the conduct of the information war against Ukraine and the lack of a holistic communicative policy of the state, the insufficient level of media culture of society [12, p. 12]. No less acute in a hybrid war is the issue of cybersecurity. In the modern world, cybernetic space increasingly serves to conduct a wide range of subversive operations: from the abduction of valuable information to acts of cyberterrorism [6, p. 18].

First of all, networks and information systems contain sensitive data and economically valuable information that increases the incentive for attacks. Attacks on information systems can have serious national consequences, such as interruptions in communication systems, leakage of confidential information, etc. [13, p. 28].

It is clear that today Ukrainian society is under constant threat of obtaining inaccurate, and sometimes harmful, information, its untimely receipt, espionage, computer crime and the like. These factors are elements of a hybrid war that contribute to the aggressor's invasion of the national consciousness of citizens, undermining national and information security.

The main components of information security are both ensuring high-quality information of citizens and free access to various sources of information, and protection from negative information influences, which together should contribute to the integrity of society. The priority task of social and state institutions should be to develop urgent effective measures to neutralize the information and sabotage activities of the Russian Federation against Ukraine and prevent its further deployment. The solution of this complex problem will protect the interests of society and the state and contribute to the realization of the right of citizens to receive comprehensive and high-quality information [14, p. 38].

Normative regulation of the formation of a single information space in Ukraine should contribute to the harmonious development of information resources, information services and the information product in the country. The importance of the development of legislation in the field of information and information security, the formation of the information society, is determined by the fact that the norms of the laws in this sphere significantly affect the legislative regulation - the formation of relations between entities in all spheres of state life.

Conclusions. In the context of Ukraine's stay in a state of war, it is possible to determine the following main directions for taking measures to protect the national information space and ensure the national information security system of Ukraine: firstly, to improve the regulatory framework in the field of state information policy, which would determine the interaction of Ukrainian law enforcement agencies with local self-government bodies, state bodies and public institutions; secondly, the establishment of a single inter-ministerial coordinating body to guide, coordinate and monitor information security measures; thirdly, to create a system of comprehensive monitoring of popular audio-visual and print media, as well as popular Internet resources; fourthly, to encourage further integrated research in the field of information security.

Public information policies in the context of globalization would be effective only if they were comprehensive, systemic and undoubtedly open, aimed at improving the interests of citizens, society and the State.

Comprehensive normative regulation of management processes it is advisable to ensure information security at the expense of systematization and harmonization of administrative legislation in the industry information security through codified regulatory legal act that will establish the basic basis of administrative and public support information security in Ukraine.

The legislative framework, combined with the restructuring of the national security system, allows for the creation of a powerful mechanism to deter external information aggression.

However, there are challenges in ensuring holistic management and protection of information resources.

Monitoring by the state of implementation is also important adopted legal norms, full financial and personnel support of structures related to the information security system, intensification of institutional reforms that meet urgent needs in this area.

References

1. Горшков М.К. Проблемы национальной безопасности в информационном обществе. *Власть*. 2014. № 11. С. 8.

2. On information: Law of Ukraine of October 02, 1992 № 2657-XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12.

3. Constitution of Ukraine of June 28, 1996 URL: http://zakon5.rada. gov.ua/ laws/show/254к/96-вр.

4. On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015: Law of Ukraine of January 09, 2007 № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?nd=1&text=%E1%E5%E7%E.

5. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

6. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.

7. Дмитренко М.А. Проблемні питання інформаційної безпеки України. *Міжнародні відносини. Серія Політичні науки*. 2017. № 17. С. 236–243.

8. On national security of Ukraine: Law of Ukraine of June 21, 2018 № 2469-VIII. URL: http://zakon.rada. gov.ua/ laws/ show/ 2469-19# n355.

9. On the Concept of the National Informatization Program: Law of Ukraine dated February 4, 1998 № 75/98-VR. URL: http:// zakon.rada.gov.ua/laws/ show/ 75/98-%D0%B2% D1%80.

10. On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015: Law of Ukraine of January 09, 2007 № 537-V. URL: http://zakon. rada.gov.ua/ laws/ show/ 537-16? nd=1&text= % E1% E5%E7%E.

11. On the State Policy Strategy for Promoting the Development of Civil Society in Ukraine and Priority Measures for Its Implementation licensing: Decree of the President of Ukraine of May 26, 2015 № 287/2015. URL: http://zakon. rada.gov.ua/laws/show/287/2015#n14.

12. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави*. Київ: Національна академія Служби безпеки України, 2018. 408 с.

13. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східно-європейського права*. 2018. № 53. С. 26–37.

14. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. *Інформаційна безпека в умовах гібридної війни*: Міжнар. наук.-практ. конф. (м. Хмельницький, 16-17 лист. 2017 р.). Хмельницький: МВС України, 2017. 50 с.

References

1. Gorshkov M.K. Problemy nacional'noi bezopasnosti v informacionnom obshhestve. *Vlast'*. 2014. № 11. S. 8.

2. On information: Law of Ukraine of October 02, 1992 № 2657-XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12.

3. Constitution of Ukraine of June 28, 1996 URL: http://zakon5.rada. gov.ua/ laws/show/254к/96-вр.

4. On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015: Law of Ukraine of January 09, 2007 № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16? nd=1&text=%E1%E5%E7%E.

5. Zolotar O.O. Informaciyna bezpeka ljudyny: teorija i praktyka: monografija. Kyiv: TOV «Vydavnychyy dim «ArtEk», 2018. 446 s.

6. Gurzhiy T. Informaciyne pravo: vyklyky gibrydnoї viyny. *Zovnishnja torgivlja: ekonomika, finansy, pravo*. 2018. № 4. S. 16–26.

7. Dmytrenko M.A. Problemni pytannja informaciynoi bezpeky Ukrainy. *Mizhnarodni vidnosyny. Serija Politychni nauky*. 2017. № 17. S. 236–243.

8. On national security of Ukraine: Law of Ukraine of June 21, 2018 № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19#n355.

9. On the Concept of the National Informatization Program: Law of Ukraine dated February 4, 1998 № 75/98-VR. URL: http://zakon.rada.gov.ua/laws/ show/ 75/98-%D0%B2%D1%80.

10. On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015: Law of Ukraine of January 09, 2007 № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16? nd=1&text=%E1%E5%E7%E.

11. On the State Policy Strategy for Promoting the Development of Civil Society in Ukraine and Priority Measures for Its Implementation licensing: Decree of the President of Ukraine of May 26, 2015 № 287/2015. URL: http://zakon. rada.gov.ua/laws/ show/287/2015#n14.

12. Bjelay S.V., Kornijenko D.M. Informaciyna bezpeka s’ogodennja – nevid’jemna skladova vojennoi bezpeky. *Aktual’ni problemy upravlinnja informaciynoju bezpekoju derzhavy*. Kyiv: Nacional’na akademija Sluzhby bezpeky Ukrainy, 2018. 408 s.

13. Voycihovs’kyy A.V. Kiberbezpeka jak vazhlyva skladova systemy zahystu nacional’noi bezpeky jevropeys’kyh krain. *Zhurnal shidno-jevropeys’kogo prava*. 2018. № 53. S. 26–37.

14. Levchenko Ju.O. Problemy protydii informaciyniy okupacii v umovah gibrydnoi viyny. Informaciyna bezpeka v umovah gibrydnoi viyny: Mizhnar. nauk.-prakt. konf. (m. Hmel’nyc’kyy, 16-17 lyst. 2017 r.). Hmel’nyc’kyy: MVS Ukrainy, 2017. 50 s.

В. П. Мороз

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: victor.moroz@npp.nau.edu.ua

Мета дослідження: *стаття присвячена аналізу особливостей інформаційної безпеки у воєнному стані.* ***Методи дослідження:*** *порівняльний аналіз окремих нормативно-правових актів і судової практики України та нормативно-правової бази і прецедентної практики у застосуванні інформаційної безпеки у воєнному стані.* ***Результати дослідження:*** *нормативне регулювання формування єдиного інформаційного простору в Україні має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні. Підвищення ефективності досліджуваних суб’єктів протидії загрозам інформаційній безпеці.* ***Обговорення:*** *проведено аналіз правових особливостей інформаційної безпеки у воєнному стані.*

В контексті перебування України у стані війни автор визначив наступні основні напрямки вжиття заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки України: по-перше, вдосконалення нормативної бази в галузі державної інформаційної політики, яка визначала б взаємодію українських правоохоронних органів із органами місцевого самоврядування, державними органами та державними установами; по-друге, створення єдиного міжвідомчого координаційного органу для керівництва, координації та моніторингу заходів інформаційної безпеки; по-третє, створення системи всебічного моніторингу популярних аудіовізуальних та друкованих засобів масової інформації, а також популярних Інтернет-ресурсів; по-четверте, заохочення подальших комплексних досліджень у галузі інформаційної безпеки.

Політика щодо публічної інформації в умовах глобалізації була б ефективною лише за умови, що вона буде всебічною, системною та, безсумнівно, відкритою, спрямованою на покращення інтересів громадян, суспільства та держави.

Доцільно забезпечити інформаційну безпеку за рахунок систематизації та гармонізації адміністративного законодавства в галузі інформаційної безпеки через кодифікований нормативно-правовий акт, який створить основи адміністративної та державної підтримки інформаційної безпеки в Україні.

Законодавча база у поєднанні з перебудовою системи національної безпеки дозволяє створити потужний механізм стримування зовнішньої інформаційної агресії.

Ключові слова: *інформаційна безпека; особливості інформаційної безпеки; військовий стан; військова агресія; вітчизняні дослідження.*