Krakowskie Studia Małopolskie
2020, nr 2 (26)

Igor Melnyk[1]

Principles of Formation of Information Policy of Ukraine In the Conditions of Hybrid War

Introduction

At the present stage, Ukraine's information policy is being implemented in a context where the concept of information sovereignty is being formed. At the same time, the information industry belongs to the strategic interests of the country and needs special attention. For Ukraine, the importance of the sphere of information policy is further conditioned by the hybrid war and information aggression that has been launched against it by Russia. The challenges of the hybrid war faced by the Ukrainian state and society have led to the formation of adequate instruments for confronting hybridity. This situation requires increased attention at the level of public administration, as the state forms a national information policy and a national security system. The hybrid warfare factor has revealed miscalculations about reformatting and implementing a modern government system that can withstand hybrid challenges at different levels.

The purpose of the study is to study the basic principles of information policy formation in Ukraine in the context of hybrid information warfare.

The research methodology involves the application of an axiological approach to the study of state information policy, which allows us

[1] Postgraduate Student at the Department of Information Policy and Digital Technologies, National Academy for Public Administration under the President of Ukraine, 482ua@i.ua, https://orcid.org/0000-0001-7257-4415.

to consider information processes as rational activities aimed at building the value paradigm of public consciousness. This approach, in the context of Russia's hybrid war against Ukraine, reveals the importance of information tools aimed at destructive influences on the public consciousness. The legal approach to state information policy means an in-depth analysis of its positive trends and overcoming the negative trends that have arisen in the legal support and real development of the information sphere.

1. Hybrid war as a challenge for globalized societies

The modern stage of development of society is characterized by the growing role of the information component, since it is the information infrastructure that performs analysis, synthesis, dissemination of information, and regulates multidimensional social relations. In addition, since the late twentieth century, a number of international conflicts have unfolded with the use of non-military influence tools, including information that have outlined the parameters of hybridity and hybrid warfare, which have become a challenge for sustainable co-existence in many countries. The basic basis in the information confrontation is «information and communication, which form the basis of all that is later regarded as information war».[2] The use of the information and communication component in the various struggles for influences and reformatting of common security strategies has made it necessary to consider the system of international public relations and a number of other key parameters of activity in a different context.

Hybrid war, which has become the most complex challenge of globalized societies, includes a wide range of financial, economic, military, strategic, socio-political, cultural, and historical components, including information and cyber war. Network technologies and modern communications have proven to be the most effective and mobile tool in hybrid wars that have been used by conflicting parties, regardless of how effective military intervention and modern weapons have been used by

[2] Kurban, O.V. (2015). Teoriya informacijnoyi vijny: bazovi osnovy, metodologiya ta ponyatijnyj aparat [Information War Theory: Basic Foundations, Methodology and Conceptual Apparatus]. *Scientific Journal Science Rise*,11/1(16), p. 97.

different states.[3] The threats of hybrid wars are universal in nature and require the development of systemic countermeasures. In fact, along with social transformations, the security of national interests began to develop quite actively. Therefore, the security sector began to expand and to acquire a completely different quality. In order to effectively counter the threat of hybrid wars and ensure a high level of security, it is an urgent need to create a comprehensive security system for modern societies, which will allow timely response to the challenges, dangers, threats that arise in society and threaten the state as a whole.[4]

In the context of a globalized information society, where conflicts of interest, competition, and power struggles and influences exist, information warfare or confrontation becomes a form of international or domestic warfare in peacetime and war. It includes a set of interrelated technical and information-psychological measures aimed at informational influence on state, public organizations, armed structures, computer networks, management systems, on the public and individual consciousness in the direction required for the opposite party, their misinformation, and violation. Normal and reliable functioning of information processes, while simultaneously protecting their information environment from the influence of the opposite party.[5]

In this context, in our opinion, it is appropriate to note that information warfare is a type of information and communication confrontation for the redistribution of zones of influence and functions within the information and communication space to achieve benefits in political, social, economic and other spheres. The most effective manipulative technologies of information and communication influence include persuasion, coercion, authorization, imitation, suggestion, conversion, etc.

[3] V.P. Gorbulin (ed.) (2017) Svitova gibrydna vijna: Ukrayinskyj front [World Hybrid War: Ukrainian Front]: Monograph. Kyiv: NISD, p. 26.

[4] Galeotti, M., Manea, O. (2015). Hybrid War as a War on Governance. Small Wars Journal, August 19. Retrieved from: http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance.

[5] Mosov, S.P., Ukhanova, N.S. (2018). Protydiya negatyvnym informacijnym vplyvam na lyudynu i suspilstvo v umovax gibrydnoyi vijny. [Counteracting Negative Information Impacts on Humans and Society in a Hybrid War]. *Informaciya i pravo*, 2 (25), p. 138.

The development and planning of hybrid war are carried out within the framework of an information warfare strategy, where the construction of an alternative reality takes place, its tactics are characterized by flexibility and diversity, acquiring new modified forms and appearing as a network-centric war, in which the modeling and programming of the necessary processes against the state mean against the state influence.[6]

The phenomenon of information warfare in humanitarian and value-based aspects and dimensions represents practically realized measures of purposeful informational influence on the mass consciousness with the purpose of transformation of established world-view, moral and value, behavioral bases in the daily activity of members of society; obtaining certain information and data for economic, political or other gain and in the direction of the interests of the hostile party engaged in such interference. Information warfare has quite advanced technologies, techniques, and techniques that are based on the use of subconscious psychology, manipulation, and more.[7]

One of the key components of hybrid war is the invasion of the information and communication space of a particular country in order to suppress resistance and to form a political state consistent with the interests of the aggressor. To do this, a variety of public opinion manipulation tools are used: launching trendy media projects, creating troll factories, bots, spreading fake news, and many other techniques that have nothing to do with honest, fact-based journalistic practice. These tools provide the same scale as cynical distortions of reality, so they are particularly dangerous for a system based on the ideas of just informing society.[8]

[6] Kuts, G.M. (2017). Priorytetni strategiyi informacijnoyi polityky u konteksti nacionalnykh interesiv Ukrainy: liberalnyj rakurs [Priority strategies of information policy in context Ukraine's national interests: a liberal perspective]. *Politychne zhyttya*, 3, p. 55.

[7] Kresina, I.O. (2019). Derzhavna informacijna polityka: aksiologichnyj ta pravovyj vymiry. [State information policy: axiological and legal dimensions]. *Mizhnarodni vidnosyny`. Seriya «Politychni nauky»*, 21. Retrieved from: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3851.

[8] Bond, M. (2007). Hybrid War: A New Paradigm for Stability Operations in the Failing States. Strategy Research Project / Colonel Margaret S. Bond. U.S. Army War College, Carlisle Barracks, Carlisle, PA. Retrieved from: https://www.semanticscholar.org/paper/Hybrid-War%3A-A-New-Paradigm-for-Stability-Operations-Bond/9eef38bab0ed2f31246fc4c0d727920ee3b328b7.

A national information policy strategy should include a multi-level and integrated approach, paying attention to such indicators as the development of the information infrastructure, the information processing industry, respect for the rights and freedoms of citizens in the information society, guaranteeing the preservation and confidentiality of information, etc.

Modern security strategies depend to a large extent on the existing system of national interests, state policy, and the actions of various actors, state and non-state actors. That is why security is understood as an integral part of social life, in which conditions are formed for the most effective implementation of the protection of the interests of man, society and the state. Safe existence is associated with the basic spheres of social life and the numerous needs of different actors, as well as certain actions in response to threats to optimize the protection of interests.[9]

The threat of hybrid wars requires special efforts on the part of state institutions to intensify international security cooperation. In modern society, the basic element of hybrid warfare is the actions of latent forces, which arise directly from the initiative and financial support of representatives of different states. The dynamics of international relations testify to the fact that today it is important to move to a comprehensive security system that is able to minimize information terrorism, cyber warfare, and cybercrime. An essential component of such a system is the state's information policy aimed at these issues.

2. Strategies of the state information policy in the conditions of hybrid war

The state information policy is aimed at the formation of the strategic course of the state in the information sphere and the management of this sphere at the level of legal regulation in order to provide citizens with proper access to information, enhance opportunities and ensure the means of its effective use, strengthen security, promote the protection of information resources, international cooperation in this field. sphere, entry of Ukraine into the world information space on an equal

[9] Galeotti, M., Manea, O. (2015). Hybrid War as a War on Governance. Small Wars Journal, August 19. Retrieved from: http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance.

basis.[10] The need for legal regulation is driven by both the ever-increasing role of information in public processes and the emergence of new opportunities for misuse of information, as evidenced by the hybrid war.

Weighted information policy is an integral part of the management system in the transition from the industrial to the information society. Information policy sets the conditions under which all managerial decisions and political activities are implemented. The state's information policy provides a reasonable conceptual framework for studying many problems at the national and regional levels.[11]

Information policy is a collection of all public laws, rules and policies that encourage, interfere with, or regulate the creation, use, storage, access and transmission and dissemination of information. Broadly speaking, information policy covers three main areas:

1. Government Creation and Dissemination – Includes state funding for research and development, as well as governmental creation of information such as economic statistics, dissemination of legislation and administrative decisions, cultural materials, etc.
2. Development, regulation and use of information infrastructure – issues such as telephony and broadcasting regulation, infrastructure for schools and libraries, security and integrity of infrastructure, etc., are addressed.
3. Institutional and legal infrastructure – includes state involvement in international treaties and organizations, privacy rules, antitrust, security, and intellectual property policies.[12]

[10] Lisovska, O.L. (2019) Priorytety derzhavnoyi informacijnoyi polityky v Ukrayini v umovax gibrydnoyi vijny [Priorities of the state information policy in Ukraine in the conditions of hybrid war]. Proceedings of Actual Problems of State Information Security Management (Kyiv, April 4, 2019), Kyiv: Nat. Acad. SBU, p. 83.

[11] Savinova, N.A. (2015). Informacijna polityka Ukrayiny u dyskursi bezpeky lyudyny i gromadyanyna. [Information Policy of Ukraine in the Discourse of Security of Man and Citizen]. Proceedings of the Actual Problems of State Information Security Management (Kyiv, March 19, 2015), Kyiv: Center for Studies, Sciences, and Period, Publications of the SB of Ukraine, p. 122.

[12] Lisovska, O.L. (2019) Priorytety derzhavnoyi informacijnoyi polityky v Ukrayini v umovax gibrydnoyi vijny [Priorities of the state information policy in Ukraine in the conditions of hybrid war]. Proceedings of Actual Problems of State Information Security Management (Kyiv, April 4, 2019), Kyiv: Nat. Acad. SBU, p. 84.

Public information policy is an important component of the foreign and domestic policy of the country and covers all spheres of life of society. The main purpose of the state information policy regarding the provision of national information resources is to create the necessary economic and socio-cultural conditions and legal and organizational mechanisms to form, develop and ensure the effective use of national information resources in all spheres of life and activity of the citizen, society and state.

The priorities of the state information policy should be to create favorable conditions for the formation, development, modernization and use of national information resources, information and telecommunications infrastructure and technologies. The state information policy should promote the development of the domestic market of information and telecommunication systems and technologies.[13] An important place in the state information policy should be given to the regulatory regulation of the functioning of international information systems in Ukraine, as well as electronic and print media. The free circulation of information and the constitutional right of citizens to search, receive, produce and disseminate it must be ensured. The problem of determining in the state information policy the principles of counteracting the external influence on the internal political situation in Ukraine.[14]

The subjects of information relations are: citizens of Ukraine, legal entities, the state. According to the Law of Ukraine "On Information", other states, their citizens and legal entities, international organizations and stateless persons may also be subjects of information relations. The following spoke on behalf of the State: President of Ukraine, Verkhovna Rada of Ukraine, Cabinet of Ministers, National Council for Television and Radio Broadcasting, and State Committee for Television and Radio Broadcasting of Ukraine. The subjects of information relations are: the docu-

[13] Spivak, K., Savruk, M. (2019). Informacijna polityka protydiyi rosijskoyi propagandy v Ukrayini [Information policy of counteracting Russian propaganda in Ukraine]. *Visnyk Lvivskogo universytetu. Seriya «Mizhnarodni vidnosyny»*, no. 46, p. 192.

[14] Savinova, N.A. (2015). Informacijna polityka Ukrayiny u dyskursi bezpeky lyudyny i gromadyanyna. [Information Policy of Ukraine in the Discourse of Security of Man and Citizen]. Proceedings of the Actual Problems of State Information Security Management (Kyiv, March 19, 2015), Kyiv: Center for Studies, Sciences, and Period, Publications of the SB of Ukraine, p. 120.

mented or publicly announced information on events and phenomena in the fields of politics, economy, culture, health care, as well as in social, environmental, international and other spheres. The object of information policy is the national information sphere, with all its components.

Since the beginning of the hybrid information war, great efforts have been made to update the legislative framework for the new vector of state information policy-making. In the context of regulatory support and regulation, a major achievement in this area was the approval of the Presidential Decree of the National Security and Defense Council Decisions: in particular, "On the Cybersecurity Strategy of Ukraine" – Presidential Decree No. 96/2016 of March 15, 2016[15]; and approval of the Information Security Doctrine of Ukraine – Presidential Decree No. 47/2017 of February 25, 2017[16]. It is these basic documents that define the priority goals and objectives in the field of information and information policy.

Thus, the Cybersecurity Strategy of Ukraine, which defines cyberspace as a separate sphere of influence with the use of modern information technologies, names as priority-vulnerable spheres that fall under the potential of such influence and the possible threat of interference the economic, scientific and technical, information sphere, as well as the area of the state management, defense, industrial and transport complexes, in general electronic communications infrastructure, security and defense sector. These areas of activity belong to the country's critical infrastructure and are potentially vulnerable. In the first place, they can be influenced by harm and disruption of information systems and net-

[15] Ukaz Prezydenta # 96 vid 15 bereznya 2016 roku «Pro rishennya Rady nacionalnoyi bezpeky ta oborony Ukrayiny vid 27 sichnya 2016 roku «Pro strategiyu kiberbezpeky Ukrayiny» [Presidential Decree No. 96 of March 15, 2016 «On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine»]. Retrieved from: http://zakon3.rada.gov.ua/laws/show/96/201.

[16] Ukaz Prezydenta # 47/2017 «Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 29 grudnya 2016 roku «Pro Doktrynu informacijnoyi bezpeky Ukrayiny». [Presidential Decree No. 47/2017 «On the Decisions of the National Security and Defense Council of Ukraine of December 29, 2016 «On the Doctrine of Information Security of Ukraine»]. Retrieved from: http://www.president.gov.ua/documents/472017–21374.

works. Similarly, information and communication technologies can be used to commit terrorist acts, in particular by violating the regular modes of operation of automated systems for managing information processes. All kinds of hacking attacks on the Internet, aimed at the penetration of information systems, theft or corruption of information or other sabotage, are becoming widespread.[17]

The adopted Cybersecurity Strategy for the first time defines the principles and outlines the main directions for its provision in the current conditions of threats and taking into account the priority of national interests of Ukraine. Thus, the main principles of cybersecurity are:

- the rule of law and respect for the rights and freedoms of man and citizen;
- observance of national interests of Ukraine;
- openness, accessibility, and security of cyberspace; extensive cooperation with civil society on cybersecurity and cyber security;
- taking adequate cyber defense measures against real and potential threats;
- the priority of preventive measures; the inevitability of punishment for cybercrime;
- development and support of national scientific, scientific, technical and industrial potential;
- international cooperation in the field of cybersecurity to develop common strategies for counteracting cyber threats, consolidate efforts to investigate and prevent cybercrime, prevent the use of cyberspace for illegal and military purposes.[18]

[17] Ukaz Prezydenta # 96 vid 15 bereznya 2016 roku «Pro rishennya Rady nacionalnoyi bezpeky ta oborony Ukrayiny vid 27 sichnya 2016 roku «Pro strategiyu kiberbezpeky Ukrayiny» [Presidential Decree No. 96 of March 15, 2016 «On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine»]. Retrieved from: http://zakon3.rada.gov.ua/laws/show/96/201.

[18] Ukaz Prezydenta # 96 vid 15 bereznya 2016 roku «Pro rishennya Rady nacionalnoyi bezpeky ta oborony Ukrayiny vid 27 sichnya 2016 roku «Pro strategiyu kiberbezpeky Ukrayiny» [Presidential Decree No. 96 of March 15, 2016 «On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine»]. Retrieved from: http://zakon3.rada.gov.ua/laws/show/96/ 2016 [in Ukrainian].

Another important document in the area of information policy and security is the Information Security Doctrine, which is based on the legal norms of the Constitution, the Laws of Ukraine, the basic requirements of the National Security Strategy of Ukraine, and other legal acts.

In accordance with the established purpose and principles, the Doctrine of Information Security aims to determine the basic principles of state policy in the field of information security, which is capable of resisting, first and foremost, the destructive and manipulative influence of the Russian Federation. At the same time, the document is based on observance of national interests, protection of national state sovereignty and independence of Ukraine, protection of democratic rights and freedoms of the person, its honor and dignity.

Considerable attention is also paid to identifying current threats to national interests in the information field and public policy priorities, although the latter is also partly determined by outlined national interests. Grouping information threats are associated with both bias and counteracting information influences, an aggressive information environment, and problems identified with regard to imperfect tools to combat these phenomena. In particular, the problematic issues are the poor formulation of strategic information policy at the state level, insufficient degree of media culture of society; dissemination of negative and threatening information that goes against the national interests of Ukraine, which calls for radical action, promotes separatist ideas, etc.[19]

The adoption of this document is conditioned by the emergence of urgent threats to national security in the information field, as well as the need to identify innovative approaches to the formation of a system of protection and development of the information space in the context of globalization and free circulation of information.

The purpose of the doctrine is to clarify the principles of the formation and implementation of state information policy, first of all, to coun-

[19] Ukaz Prezydenta # 47/2017 «Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 29 grudnya 2016 roku «Pro Doktrynu informacijnoyi bezpeky Ukrayiny». [Presidential Decree No. 47/2017 «On the Decisions of the National Security and Defense Council of Ukraine of December 29, 2016 «On the Doctrine of Information Security of Ukraine»]. Retrieved from: http://www.president.gov.ua/documents/472017–21374.

teract the destructive information influence of the Russian Federation in the conditions of its hybrid war. The doctrine identifies four key public policy priorities in the information field: 1) ensuring information security; 2) ensuring the protection and development of the information space of Ukraine, as well as the constitutional right of citizens to information; 3) openness and transparency of the state to the citizens; 4) formation of a positive international image of Ukraine [1, p.51].[20]

In the context of the adopted laws, which will contribute to the further formation of information policy, the basic principles of democracy and governance are defined, since the issue of information security becomes one of the urgent for the construction and functioning of the relevant information infrastructure, which requires legislative regulation of these issues.

Conclusions

The analysis of the study of the basic principles of information policy-making in the context of hybrid warfare influences the necessity to change the approaches to the policy of state power institutions, which should have the maximum ability to integrate in response to hybrid challenges. Adapting to the threats of hybrid warfare requires state officials to significantly enhance their professional skills, enabling them to develop concepts of rapid response across a broader range of capabilities and to facilitate full interaction between the various levels of government. In the course of reforming the organizational and legal mechanisms for implementing the state information policy and mechanisms for managing the development of information infrastructure, it is necessary to take into account such general tendencies as globalization, the convergence of information and telecommunications technologies, their dynamic and large-scale development and implementation in all spheres of public life, differentiation of public administration functions in the field of information and communication technologies and their delegation to separate state bodies, decentralization and deregulation of power, a broad in-

[20] Berislavska, O.M. (2017). Osoblyvosti informacijno-pravovoyi polityky Ukrayiny v umovax «gibrydnoyi vijny». [Features of information and legal policy of Ukraine in the conditions of «hybrid war»]. *Prykarpatskyj yurydychnyj visnyk*, 2 (17), p. 51.

troduction to management activities of modern management methods, especially strategic management, public management, network governance and so on.

Bibliography

Berislavska, O.M. (2017). Osoblyvosti informacijno-pravovoyi polityky Ukrayiny v umovax «gibrydnoyi vijny». [Features of information and legal policy of Ukraine in the conditions of «hybrid war»]. *Prykarpatskyj yurydychnyj visnyk*, 2 (17).

Bond, M. (2007). Hybrid War: A New Paradigm for Stability Operations in the Failing States. Strategy Research Project / Colonel Margaret S. Bond. U.S. Army War College, Carlisle Barracks, Carlisle, PA. Retrived from: https://www.semanticscholar.org/paper/Hybrid-War%3A-A-New-Paradigm-for-Stability-Operations-Bond/9eef38bab0ed2f312 46fc4c0d727920ee3b328b7.

Galeotti, M., Manea, O. (2015). Hybrid War as a War on Governance. Small Wars Journal, August 19. Retrieved from: http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance.

Gorbulin V.P. (ed.) (2017) Svitova gibrydna vijna: Ukrayinskyj front [World Hybrid War: Ukrainian Front]: Monograph. Kyiv: NISD (in Ukrainian).

Gurzhiy, T. (2018). Informacijne pravo: vyklyky gibrydnoyi vijny. [Information Law: The Challenges of Hybrid War]. *Zovnishnya torgivlya: ekonomika*, *finansy*, *pravo*, no. 4.

Kresina, I.O. (2019). Derzhavna informacijna polityka: aksiologichnyj ta pravovyj vymiry. [State information policy: axiological and legal dimensions]. *Mizhnarodni vidnosyny`. Seriya «Politychni nauky»*, no. 21. Retrieved from: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3851.

Kurban, O.V. (2015). Teoriya informacijnoyi vijny: bazovi osnovy, metodologiya ta ponyatijnyj aparat [Information War Theory: Basic Foundations, Methodology and Conceptual Apparatus]. *Scientific Journal Science Rise*,11/1(16), pp. 95–100.

Kuts, G.M. (2017). Priorytetni strategiyi informacijnoyi polityky u konteksti nacionalnykh interesiv Ukrainy: liberalnyj rakurs. [Priority strategies of information policy in context Ukraine's national interests: a liberal perspective]. *Politychne zhyttya*, no. 3.

Lisovska, O.L. (2019) Priorytety derzhavnoyi informacijnoyi polityky v Ukrayini v umovax gibrydnoyi vijny [Priorities of the state information policy in Ukraine in the conditions of hybrid war]. Proceedings of Actual Problems of State Information Security Management (Kyiv, April 4, 2019), Kyiv: Nat. Acad. SBU.

Mosov, S.P., Ukhanova, N.S. (2018). Protydiya negatyvnym informacijnym vplyvam na lyudynu i suspilstvo v umovax gibrydnoyi vijny. [Counteracting Negative Information Impacts on Humans and Society in a Hybrid War]. *Informaciya i pravo*, 2 (25).

Savinova, N.A. (2015). Informacijna polityka Ukrayiny u dyskursi bezpeky lyudyny i gromadyanyna. [Information Policy of Ukraine in the Discourse of Security of Man and Citizen]. Proceedings of the Actual Problems of State Information Security Management (Kyiv, March 19, 2015), Kyiv: Center for Studies, Sciences, and Period, Publications of the SB of Ukraine.

Spivak, K., Savruk, M. (2019). Informacijna polityka protydiyi rosijskoyi propagandy v Ukrayini [Information policy of counteracting Russian propaganda in Ukraine]. *Visnyk Lvivskogo universytetu. Seriya «Mizhnarodni vidnosyny»*, no. 46.

Ukaz Prezydenta # 47/2017 «Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 29 grudnya 2016 roku «Pro Doktrynu informacijnoyi bezpeky Ukrayiny». [Presidential Decree No. 47/2017 «On the Decisions of the National Security and Defense Council of Ukraine of December 29, 2016 «On the Doctrine of Information Security of Ukraine»]. Retrieved from: http://www.president.gov.ua/documents/472017–21374.

Ukaz Prezydenta # 96 vid 15 bereznya 2016 roku «Pro rishennya Rady nacionalnoyi bezpeky ta oborony Ukrayiny vid 27 sichnya 2016 roku «Pro strategiyu kiberbezpeky Ukrayiny» [Presidential Decree No. 96 of March 15, 2016 «On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine»]. Retrieved from: http://zakon3.rada.gov.ua/laws/show/96/ 2016.

Summary

The purpose of the article is to explore the basic principles of information policy formation in Ukraine in the context of hybrid information warfare; identification of features and problems of information policy and its impact on the public administration system. The results of the study show that since the beginning of Russia's armed aggression against Ukraine and the widespread hybrid information war, the state's information policy has changed its vectors and priorities. Confirmation of this was the adoption of a number of legislative documents, which identified the external enemy of the aggressor and outlined directions for the protection of national interests. It is analyzed that one of the main tasks in the information confrontation of the hybrid war is the formation of appropriate information policy and information security. It was pointed out that in the conditions of a hybrid war, a systematic approach should be devised to adequately respond to the state's power structures to the challenges related to information confrontation. In order to minimize the spread of manipulative influences in the national information space, the formation of practical mechanisms for implementing the country's information policy, establishing communication with civil society and raising the overall level of media literacy of society is a necessary question.

Keywords: hybrid war, information war, information policy, public administration, manipulation, information security, national interests, internet network, information space