

UDC: 35:316.77:341.1/8

DOI: <https://doi.org/10.32689/2617-2224-2019-18-3-143-157>

Hološanova Natalia Viktorivna,

Ph.D. student of the 4th year of the Department of Political Science and Philosophy, Kharkiv Regional Institute of the National Academy of Public Administration under the President of Ukraine, 61000, Kharkiv, avenue Moscow, 75, tel.: +38 097 946 90 79, +38 099 146 60 19, e-mail: natalya041162@gmail.com

ORCID: 0000-0002-6729-2226

Голованова Наталія Вікторівна,

аспірант 4 курсу кафедри політології та філософії, Харківський регіональний інститут Національної академії державного управління при Президентові України, 61000, Харків, просп. Московський, 75, тел.: +38 097 946 90 79, +38 099 146 60 19, e-mail: natalya041162@gmail.com

ORCID: 0000-0002-6729-2226

Голованова Наталья Викторовна,

аспірант 4 курса кафедры политологии и философии, Харьковский региональный институт Национальной академии государственного управления при Президенте Украины, 61000, Харьков, просп. Московский, 75, тел.: +38 097 946 90 79, +38 099 146 60 19 e-mail: natalya041162@gmail.com

ORCID: 0000-0002-6729-2226



INFORMATION POLICY OF UKRAINE AS AN EUROPEAN STATE IN CONDITIONS OF CURRENT THREATS (ARCHITECTURE APPROACH)

Abstract. The sources of the anthropocentric matrix of concepts and ideas in the information sphere are presented. The challenges and threats to the information sphere of Ukraine are given. The external and internal factors of these threats are specified. Specific facts of threats in the world are considered. The peculiarities of the European countries' regulatory policy in the area of counteracting threats and legal security of information security as a sub-branch of information law are analyzed. The landscape of the threat of information security 2019 is defined. The mechanism of ethnic lobbying as a tool of soft law is given. It's shown that the tendency of citizens' strivings is not to safety, but to freedom. It is revealed that security measures are simultaneously factors limiting the freedom of citizens. The importance of launching the anti-Ukrainian language counterac-

tion system in the area of the Anti-terrorist operation in the East of Ukraine in April 2018 and activities within the framework of the Framework Cooperation Program of Ukraine with the Council of Europe and the European Union was emphasized. To counter propaganda, it is proposed to apply and improve the universal international legal regulation of media space, to build a single European space. The content of Ukraine's national interests according to the Doctrine of Information Security of Ukraine is determined. Objects of national interests in the information sphere are called information, information infrastructure and status of the subject in the information sphere. It is emphasized on the value-filling of information policy of the state. The realization and survival of an individual, society and state are defined as the goal of information policy in the context of modern threats. State security, economic prosperity, the development of society and the harmonious existence of the country in the global context are indicated as the result of effective information policy. It is suggested to rely on the state-owned approaches inherent in historical Kyiv and the modern Ukrainian state.

Keywords: geopolitical confrontation, propaganda, manipulation, fake, cyber troops, landscape threats, sources of soft law, ethnic lobbying, national values, European and national security systems, information security, information infrastructure.

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ ЯК ЄВРОПЕЙСЬКОЇ ДЕРЖАВИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ (АРХЕТИПНИЙ ПІДХІД)

Анотація. Представлено джерела антропоцентричної матриці понять та ідей в інформаційній сфері. Зазначені виклики і загрози інформаційній сфері України. Уточнені зовнішні та внутрішні чинники цих загроз. Розглянуті конкретні факти загроз у світі. Проаналізовані особливості регуляторної політики європейських держав у напрямку протидії загрозам та правового забезпечення інформаційної безпеки як підгалузі інформаційного права. Визначений ландшафт загрози інформаційної безпеки 2019 р. Приведений механізм етнічного лобізму як інструменту “м’якого” права. Наголошено на тенденції прагнення громадян не до безпеки, а до свободи. Виявлено, що заходи безпеки є одночасно факторами обмеження свободи громадян. Підкреслено важливість запуску системи протидії антиукраїнському мовленню в зоні проведення антитерористичної операції на Сході України у квітні 2018 р. та заходів у межах Рамкової програми співробітництва України з Радою Європи та Євросоюзом. Для протидії пропаганді запропоновано застосовувати та вдосконалювати універсальне міжнародно-правове регулювання медіапростору, будувати єдиний європейський простір. Визначено зміст національних інтересів України згідно з Доктриною інформаційної безпеки України. Об’єктами національних інтересів у інформаційній сфері названо інформацію, інформаційну інфраструктуру і статус суб’єкта в інформаційній сфері. Наголошено на ціннісному наповненні інформаційної політики держави. Реалізацію і виживання окремої особи, суспільства та держави ви-

значено як мету інформаційної політики в умовах сучасних загроз. Безпеку держави, економічне процвітання, розвиток суспільства і гармонійне існування країни у світовому контексті зазначено як результат ефективної інформаційної політики. Запропоновано спиратися на державницькі підходи, притаманні історичному Києву та сучасній українській державі.

Ключові слова: геополітичне протистояння, пропаганда, маніпулювання, фейк, кібервійська, ландшафт загрози, джерела “м’якого” права, етнічний лобізм, національні цінності, системи європейської і національної безпеки, інформаційна безпека, інформаційна інфраструктура.

ИНФОРМАЦИОННАЯ ПОЛИТИКА УКРАИНЫ КАК ЕВРОПЕЙСКОГО ГОСУДАРСТВА В УСЛОВИЯХ СОВРЕМЕННЫХ УГРОЗ (АРХЕТИПИЧЕСКИЙ ПОДХОД)

Аннотация. Представлены источники антропоцентрической матрицы понятий и идей в информационной сфере. Указаны вызовы и угрозы информационной сфере Украины. Уточнены внешние и внутренние факторы этих угроз. Рассмотрены конкретные факты угроз в мире. Проанализированы особенности регуляторной политики европейских государств в направлении противодействия угрозам и правового обеспечения информационной безопасности как подотрасли информационного права. Определен ландшафт угрозы информационной безопасности 2019 г. Приведен механизм этнического лоббизма как инструмента “мягкого” права. Отмечены тенденции стремления граждан не к безопасности, а к свободе. Показано, что меры безопасности являются одновременно факторами ограничения свободы граждан. Подчеркнута важность запуска системы противодействия антиукраинской речи в зоне проведения антитеррористической операции на Востоке Украины в апреле 2018 г. и мероприятий в рамках Рамочной программы сотрудничества Украины с Советом Европы и Евросоюзом. Для противодействия пропаганде предложено применять и совершенствовать универсальное международно-правовое регулирование медиапространства, строить единое европейское пространство. Определено содержание национальных интересов Украины согласно Доктрине информационной безопасности Украины. Объектами национальных интересов в информационной сфере названы информация, информационная инфраструктура и статус субъекта в информационной сфере. Отмечена важность ценностного наполнения информационной политики государства. Реализация и выживание отдельной личности, общества и государства определены как цель информационной политики в условиях современных угроз. Безопасность государства, экономическое процветание, развитие общества и гармоничное существование страны в мировом контексте указаны как результат эффективной информационной политики. Предложено опираться на государственные подходы, присущие историческому Киеву и современному украинскому государству.

Ключевые слова: геополитическое противостояние, пропаганда, манипулирование, фейк, кибервойска, ландшафт угрозы, источники “мягкого” пра-

ва, этнический лоббизм, национальные ценности, системы европейской и национальной безопасности, информационная безопасность, информационная инфраструктура.

Target setting. Regarding the current geopolitical situation and policies of European countries in terms of the use of military-political mechanisms for the provision of security and defense, the issue now stands for the construction of a new system of European and national security, which should include all existing security and defense institutes for a clear separation of their functions. Traditional ideas about the symbols of power and ways of achieving world domination change. Previously, it was about land, air and sea spaces, now it is about updating the role of information space and a new field of geopolitical confrontation – the information sphere. Therefore, the problem of modern challenges and threats to Ukraine's information security is extremely relevant. The Internet has a dominant role, the undisputed leader of the development of which is the United States. However, today there's an opinion on the need to optimize the paths of global information flows. That is, we can already say that the world is on the verge of a new battle for the control over the information space and the "transportation of information".

"Of course, in today's geopolitical conditions, the importance of the information factor increases. There is a clear tendency to increase the role of information resources of states in the overall system of defense capabilities. Its most important elements are information systems and means of strategic preven-

tion, control of troops and weapons, navigation, intelligence, and electronic warfare... Thus, geopolitical transformations determine the nature of cooperation and confrontational relations in the 21st century. The main field of confrontation is the information space of the global, regional and national levels. Geopolitical conditions determine the military information policy of the state in the most important spheres of geopolitical rivalry and confrontation" [1, p. 44–45].

The aggressive external environment was put forward by Ukraine in the years 2014–2019, first of all in the face of the state's information policy, new threats.

Analysis of basic research and publication. Some researchers identify the main types of threats to information security as follows:

- large-scale informatization, increasing the dependence of the military sector on modern information technologies, simplifying communications and accelerating the flow of information flows;
- formation of information sphere not bound to state borders;
- transforming the information space of Western powers into a single global information space, where the United States and EU countries play a dominant role in controlling information flows;
- the formation of a global information infrastructure based on the

Internet, which can be considered as strengthening the spatial interdependence of states;

- displacement of domestic news agencies, mass media from the internal information market and strengthening the dependence of the spiritual, economic and political spheres of public life in Ukraine from foreign information structures;

- manipulation of information, fake, etc.;

- development of information weapons or its elements in almost 120 countries of the world (according to American experts);

- Information influence of foreign political, economic, military and information structures on the development and implementation of the foreign policy of the state;

- spread abroad of misinformation about Ukraine's foreign policy;

- violation of the rights of citizens and legal entities in the information sphere of Ukraine and abroad;

- attempts to unauthorized access to information and influence on information resources, information infrastructure of state authorities, which implement the state foreign policy, Ukrainian representations and organizations abroad, and representations of Ukraine at international organizations [1, p. 45–52].

We have the following major groups of threats: information, information and technology, electronic control over life, the use of new information technologies for political purposes.

The most significant are the following:

- threats connected with destruction or degradation, internal and exter-

nal, information and cultural basis of society, the main custodian of which is the system of education and upbringing of new generations of society;

- threats associated with the destruction or degradation of a productive information subsystem of society are scientific, technical, analytical, and ideological centers that create or import relevant information products and information technologies.

In the system of ensuring national security of the state, US military researchers Jagger Richard and George Barber consider the following triad:

- national values in the information sphere;

- national interests in the information sphere;

- national goals in the information sphere.

According to the Doctrine of Information Security of Ukraine, Ukraine's national interests in the information sphere are:

- observance of constitutional rights and freedoms in the possibility of obtaining information, preservation and strengthening of values;

- representing Ukraine in the international environment and informing Ukrainian citizens about state information policy;

- development of modern information technologies;

- protection of information resources [2].

Objects of national interests in the information sphere are the information, information infrastructure and the status of the subject in the information sphere. The state information policy is aimed at the realization and survival of the individual, society and the state.

For the state as a whole, this means its security, economic prosperity, the development of society and the harmonious existence of the country in a global context.

Value added information policy is important. It's made, according to C. Lerci and A. Said, by individual citizens, society, state, socially interested groups and government [3, p. 11]. On the basis of values, the priorities of information policy are formed. The formation of priorities should be of a systemic nature.

M. Weber believes that the system of values is determined primarily by the historical epoch [4, p. 64].

B. Gogwood and L. Gang consider national values as beliefs, morals, standards, and other specific benchmarks that influence policy making at all levels, since they create contexts of deterrence, influence, and incentive for parties to take decisions in one or another process [5, p. 160].

According to the work of V. Gorbunin and A. Kachinsky, the core value consolidating society is national security, spiritual heritage, prosperity, international relations, patriotism and social justice [6, p. 107].

The purpose of the article is to find out the directions and principles of information policy of Ukraine as a European state in the context of modern threats.

The statement of basic materials. Seeing that fact and truth are relative concepts, and approaches are created by man, in our opinion, it's important to immediately determine the matrix of concepts and ideas.

We define the matrix of concepts and ideas as anthropocentric, that is, we

will take as a basis the fact that man is the center of the universe and the purpose of all events that it was designed and created by God in His image and likeness.

Primary sources and first legislators became ancient sacred books are:

- Bible (XV century BC – I century AD);
- Tanah;
- Quran;
- Trypitka (Pali canon);
- Go away;
- V-Jing;
- Tao tsan, Chuang-tsi.

Biblical commandments of bliss are:

- Blessed [happy] poor in spirit [need the Spirit, realize the need for spiritual self-perfection – are spiritually perfected], because theirs is the kingdom of heaven.
- Blessed are sorrowful, for they will be comforted.
- Blessed are the meek, for they inherit the earth.
- Blessed are hungry and thirsty for the truth, for they will be filled.
- Blessed are the merciful, for they will be merciful.
- Blessed are the pure in heart, for they will see God.
- Blessed peacemakers, for they will be called the sons of God.
- Blessed are persecuted for righteousness, for theirs is the kingdom of heaven.
- Blessed are you, when they will disgrace you and persecute and utterly wickedly speak evil of Me. Rejoice and be glad, for your reward is great in heaven! For so persecuted also the prophets that were before you (Matthew 5: 3-12).

The challenges and threats to Ukraine's information security are: the presence of problems in the formation and implementation of state information policy, adequate to the challenges and threats to Ukraine's information security; the lack of effective information and analytical support for the leadership of the state and state authorities; attempts to interfere in the internal affairs of Ukraine by foreign states, organizations and groups; use of information space by foreign states for the purpose of informational or military aggression; dissemination of negative informational and technological influences on human consciousness; the creation of foreign powers of cyber troops, cyber units in traditional genera of troops, the development of new types of information weapons and weapons of a cybernetic nature; the dependence of the national information infrastructure on foreign manufacturers of high-tech products; improper level of informatization of the activities of state bodies, local governments and other areas of information activity; imperfection of the state strategy and the system of counteraction to external information expansion into the national information space; restriction of freedom of speech and dissemination in the media of a cult of violence, cruelty, disdainful attitude towards human and national dignity, provoking confrontation in society; the implementation of software and mathematical tools that violate the functioning of information systems, radio-electronic locking of communication and control, the inclusion in the software of hidden malware functions; the use of unlicensed and uncertified software, the lack of prio-

rity development of national software; insufficient level of development of national information infrastructure, low competitiveness of domestic high-tech production of information technologies, information products and services; insufficient reliability of information and telecommunication systems for the collection, processing and transmission of information in emergencies, the absence of effective national and local notification systems, early warning and emergency response; manifestations of unauthorized access to personal data and information resources of state authorities and local self-government; violation of the established procedure for collecting, processing, storing and transmitting data; illegal interception of information in telecommunication networks, separatist and other criminal manifestations in the information sphere; inconsistency of legal responsibility with contemporary challenges and threats to information security; the lack of effective democratic control over the activities of the subjects of ensuring information security, the security of the national information infrastructure and information space of Ukraine. The vast majority of these threats are inherent in different countries, but in the conditions of socio-cultural and economic transit experienced by the Ukrainian state and society, these threats are actualized and aggravated.

Contemporary challenges to the information security of Ukraine, as V. Konakh and O. Lazorenko rightly point out, are caused both by internal and external factors. The domestic ones are most associated with the backwardness of information technology in Ukraine from the leading countries of

the world, the inadequacy of government bodies and legislation in the information sphere, as well as indifference, low level of understanding and professional responsibility of both groups and citizens who are currently conducting its activity in the information space of Ukraine. External – with the efforts of foreign actors to influence the world and domestic information space in order to provide their own interests” [7, p. 74–77].

In this situation, the issues of information security first of all, its informational and psychological component, are put on the foreground. Today, the fact that the more information the state possesses, the more likely it is (the more equal conditions) that it will attain strategic advantages in the information space. This is especially relevant for determining the role and place of Ukraine in the current conditions of information globalization.

What is the experience of information security policy of foreign countries?

CM document (2002) 49 proclaims five key principles of NATO’s security policy [8]:

- “principle of latitude”;
- “principle of depth”;
- “principle of centralization”;
- “principle of access control”;
- “the principle of personal control”.

An important task for NATO is to prevent acts of aggression in cyberspace, as well as to the cyber defense of individual member states.

P. Kornis of the London Royal Institute of Foreign Affairs offers the following classification of information threats: hacker-alone attacks; organized crime in networks; ideological and political

extremism; information aggression of states [9].

The experience of Austria, Switzerland, Finland and Ireland in data protection, early detection of cyberthreats and cyberattacks, critical infrastructure enhancement, cyber-rush, cyber-espionage and cyber-sabotaging is helpful. [10]

The most important aspect of the information security of all EU countries without exception is protection of personal data, the principles of which are defined by Directive 95/46 / EC “On Protection of Individuals in the Context of the Processing of Personal Data and the Free Circulation of Such Data”. The document simultaneously declares the desire for free movement of information between EU member states. The new Personal Data Protection (GDPR) rules enhance the storage of personal data and impose a more severe penalty for late-reporting of the data stream [11]. Active implementation of the new rules is Romania, Bulgaria, Moldova.

According to the “European Criteria for Information Technology Security” (1991), for the EU countries, security and integrity of information resources are important for the EU countries, and the CIA Triad is the main characteristics of information security is confidentiality, integrity and accessibility. Problems are uncoordinated national approaches, as well as the lack of a European-level partnership between the public and private sectors.

Germany is developing the methods of “active defense”. France also has a similar drive.

Poland, the Czech Republic and Slovakia have developed new legislation to

protect classified information on new principles.

Hungary adapted to the requirements of NATO the former legislation on the protection of state and official secrets and the first of the post-socialist countries adopted a legal act on the protection of personal data.

The national cyber security strategy was adopted in Croatia.

“According to long-term forecasts, the prospects for global development will determine the global regrouping of forces as a result of information progress in the US, EU, Japan, China, India and Russia. It is planned to develop three powerful geostrategic and informational “centers of the world”: the American (US), European (European Union) and Asian (China, India, Japan). The Russian Federation is trying to become a similar center of information influence in modern conditions. Ukraine in this international design occupies a special place due to its geopolitical location” [1, p. 46].

“We live in a world where states (and large corporations) translate in their favor any technical novelties that at first seem quite democratic. Everything is gradually becoming controlled by the state or a large business capable of paying for controllability costs” [12].

G. Pocheptsov gives examples of the victory of the states over potentially dangerous tendencies for them.

Social networks China, Israel, Russia, and the USA have made it manageable.

Reviews in online stores, for the most part, became fake.

Hollywood has a representation of American military and intelligence

agencies that help in filming the right movies.

In Britain the behavior of football fans, as well as protesters is seriously studied, in the United States the behavior of the crowd and looking for automatic recognition of patterns of abnormal passenger behavior at the airport are seriously studied.

Recognition and observation systems are located on the streets in the phones of citizens.

The system was also work with mass consciousness, where primacy belongs to China. China has created a system of “de-extremism” to rebuild its Uighur Muslim population, as well as a system of social credit for all: people gain points for good behavior (for example, visit their old parents) or lose them. With a small amount of points it’s impossible to borrow or buy a plane ticket. There’s an application for the phone which states that next is the debtor.

It’s also an example of interference in the election of other states.

Regulatory policy of European states, in particular in the field of broadcasting in the face of information threats, takes into account the criteria of accuracy, impartiality, independence, responsibility and the establishment of standards as criteria for approaches.

The world that technically goes forward loses its social orientations behind. This is clearly demonstrated by giants like Facebook, when well-designed for making money to its creators, the technical model has come into conflict with moral standards, with people whose personal information is a resource, where Facebook makes its money. And since this business model is based on monopoly giants,

they try to dictate these rules to everyone.

Concerning Fake's, G. Pocheptsov asserts that the answer to them or the complaint is post-factorial journalism, it is not as effective as it covers a wider audience or fake covers one audience and the answer is different. In his opinion, the Ukrainian counter-narrative [13] is a warning blow needed.

The legal security of information security is a subset of information law. This sub-sector acquires special significance in the conditions of negative external influence on information space.

The state of information security is influenced by:

- foreign policy situation in the world;
- internal political situation in the state;
- presence of potential threats;
- the level of development of the media space of the country.

In 2015 "Ukraine ranked 5th in the world ranking of risk of collision with Web threats. In the third quarter of 2015, one-third (33,7 %) of antivirus users encountered threats that spread through the Internet. The problem is the lack of software updates and the use of pirated software. About 17 % of the infections were committed to outdated WindowsXP users. Encryption programs that require money after encrypting files that can not be accessed without a special key are also dangerous. A major problem is social engineering. Malicious people are spreading their programs through social networks, phishing and malicious sites" [14, p. 87].

The terrain of the threat of information security is constantly evolving.

Each year, the Information Security Forum (ISF), a nonprofit association that explores and analyzes security and risk management issues on behalf of its members, publishes the "Danger" report to present the prospect of the greatest security threats for two years.

Here are the biggest threats until 2019:

- excessive dependence on complication and sensitivity (unreliability) of communication;
- actions of criminal syndicates;
- loss of trust in information;
- the problem of observance of legislative norms [15].

Under conditions of modern threats, ethnic lobbying becomes a special value, which becomes an instrument for building up the "soft power" of Ukraine [16, p. 280–283].

At the same time, researchers note the tendency of citizens to strive not for safety but for freedom. At the same time, security measures are simultaneously factors limiting the freedom of citizens [17; 18].

The peculiarities of the philosophy of Kyivan Rus right to become:

- syncretism;
- variety of approaches and polyphony;
- cordocentrism and wisdom;
- kyivocentrism;
- jerusalemocentrism and travel.

The role of the Ukrainian capital is decisive in the nation-forming, historical-cultural, spiritual-value, human-dimensional, linguistic and geopolitical aspects. Kyiv itself, as the capital, is the center that cements the unity of the state and provides harmonious coexistence of the regions of Ukraine, gives the mental field, the media space of

the country the national spiritual and aesthetic qualities inherent in the best personalities and embodied in the best examples of science and art. Prognostically, Kyiv itself can be a model of state-owned approaches.

On April 19, 2018, Ukraine announced *the launch of a system to counter anti-Ukrainian speech* in the area of the Anti-Terrorist Operation in the East of Ukraine, developed with the active participation of the Ministry of Information Policy, the State Service for Special Communications and Information Protection, the Committees of the Verkhovna Rada on National Security and defense and freedom of speech and information policy, the National Council on Television and Radio Broadcasting, the Security Service of Ukraine and other bodies of state power.

Among the activities within the framework of the Framework Program of Co-operation (RPM) of Ukraine with the Council of Europe and the EU, the project “Freedom of the Media in Ukraine” – creation of low-power broadcasting (community broadcasting) and control over observance of legislation on language quotas on radio and television.

The conclusions of the European Parliament Resolution of 23 November 2016 on EU Strategic Communications for Combating Propaganda (2016/2030 (INI) [19] are effective.

Conclusions. The agenda for the information policy of Ukraine as a European state in the context of modern threats is:

- universal international legal regulation of the media space, the construction of a single European space, taking into account the space of the world;

- provision of high-quality content of television and radio programs, participation in the programs of scientists, specialists, experts, compliance with the broadcasting code, provision of benefits in the part of retransmission to public broadcasting programs;

- elimination of stereotypes;

- rhetoric of peace;

- the development of translation activities and the inclusion in the List of television and radio programs adapted for broadcasting in Ukraine, showing films of the countries of the European Union and other countries of the world;

- development and support of Ukraine’s communications with the world, in particular the dialogue of intellectual elites of experts and experts in the world media space, initiation of the All-Ukrainian, All-European and World-wide linguistic dialogue;

- development of the cultural and educational space as a part of the social space and media space of Ukraine of the metamodern era and popularization of the study of every Ukrainian of its own history, ideally, of universal humanitarian education; recognition by universities and academies of the status of centers of knowledge and sources of innovative ideas in society;

- introduction of non-violence policy in society;

- the introduction in practice of the principles of New Public Governance, curbing “soviet” methods and approaches in information policy, the introduction of subjective-subjective social relations, the transition from the web of hierarchical connections to the network of interconnections and the power of creativity;

- appeal to national memory, to the philosophical ideas of Kyivan Rus, to the ideas of travel, cordocentrism and openness;

- attention to the context of events, texts, statements; taking into account the ideas and thoughts of the single (researchers with a specific style of work in solitude and independent conditions);

- the desire to know Ukraine and Ukrainian as such;

- involvement of methods of linguistics, neuroscience, artificial intelligence, approaches of post-classical sciences;

- overcoming the enthusiasm of lawmaking;

- recognition of truth as the foundation of a humanistic world outlook.

REFERENCES

1. *Pylypchuk, V., Dzoban, O.* (2014). Hlobalni vyklyky y zahrozy natsionalnii bezpetsi v informatsiinii sferi [Global challenges and threats to national security in the information sphere]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy – Bulletin of the National Academy of Legal Sciences of Ukraine*, 3 (78), 43–52. Retrieved from http://nbuv.gov.ua/UJRN/vapny_2014_3_6 [in Ukrainian].
2. Ukaz prezidenta Ukrainy “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku “Pro Doktrynu informatsiinoi bezpeky Ukrainy” vid 25 liutoho 2017 roku, № 47/2017 [Decree of the President of Ukraine “On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016 “On the Doctrine of Information Security of Ukraine” from February 25 2017, № 47/2017]. www.president.gov.ua. Retrieved from <https://www.president.gov.ua/documents/472017-21374> [in Ukrainian].
3. *Lerche Ch., Said A.* (1979). *Politics Concepts of International in Global Perspective*. Englewood Cliffs: Prentice-Hall [in English].
4. *Weber M.* (1994). *Izbrannoe. Obraz obshchestva* [Selected. The image of society]. Moscow: Yurist [in Russian].
5. *Gogwood B., Gan L.* (2004). *Analiz polityky dlia realnoho svitu* [Analysis of politics for the real world]. (A. Oliinyk, Trans). V. Tertychko (Eds.). Kyiv: Vyd-vo Solomii Pavlychko “Osnovy” [in Ukrainian].
6. *Horbuin V., Kachynskiji A.* (2009). *Zasady natsionalnoi bezpeky Ukrainy* [Principles of National Security of Ukraine]. Kyiv: Inter-tekhnohiiia [in Ukrainian].
7. *Konakh V., Lazorenko O.* (2014). *Zahrozy ta vyklyky natsionalnym interesam Ukrainy v informatsiinii sferi v umovakh hlobalizatsii* [Threats and challenges to the national interests of Ukraine in the information sphere in the conditions of globalization]. *Stratehichni priorytety – Strategic priorities*, 2, 73-78. Retrieved from http://nbuv.gov.ua/UJRN/spa_2014_2_13 [in Ukrainian].
8. *Roberts Al. S.* (2002). *Entangling Alliances: Nato’s security of information policy and the entrenchment of State Secrecy*. *Cornell international law journal*, 26(2). Retrieved from https://www.researchgate.net/publication/228222455_Entangling_Alliances_NATO’s_Security_Policy_and_the_Entrenchment_of_State_Secrecy [in English].
9. *Cornish P.* (2014). *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacs*. Brussels: European Parliament [in English].
10. *National Strategy for Switzerland’s protection against cyber risks.* (2012). www.enisa.europa.eu. Retrieved from <https://www.enisa.europa.eu>.

- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf [in English].
- 2018 reform of EU data protection rules (n.d.). ec.europa.eu. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [in English].
 12. *Pocheptsov H.* (February 4, 2019). Svit bazuietsia na informatsii ta buduetsia neiu [World is based on information and is being built by it]. detector.media. Retrieved from <https://detector.media/withoutsection/article/144566/2019-02-04-svit-bazuetsya-na-informatsii-ta-buduetsya-neyu/> [in Ukrainian].
 13. *Pocheptsov H.* (February 13, 2019). Kak ubit feyk, ili gde ukrainskie kontrnarrativy [How to kill a fake, or where Ukrainian counter-narratives are]. hvylya.net. Retrieved from <https://hvylya.net/analytics/society/kak-ubit-feyk-ili-gde-ukrainskie-kontrnarrativyi.html> [in Ukrainian].
 14. *Platonenko A.* (2015). Suchasni zahrozy informatsiinoi bezpeky dlia derzhavnykh ta pryvatnykh ustanov Ukrainy [Modern threats of information security for state and private institutions in Ukraine]. Suchasnyi zakhyst informatsii — Modern Information Security, 4, 86–90. Retrieved from <http://journals.dut.edu.ua/index.php/dataprotect/article/view/428> [in Ukrainian].
 15. *Olavsrud T.* (March 28, 2017). 9 biggest information security threats through 2019. www.itworld.com. Retrieved from <https://www.itworld.com/article/3185725/9-biggest-information-security-threats-through-2019.html> [in English].
 16. *Musiienko I. V.* (2013). Etnichniy lobizm yak instrument naroshchuvannia “miakoi syly” Ukrainy [Ethnic lobbyism as a tool for “soft power” expansion in Ukraine]. Hileia, 77(10), 280–283 [in Ukrainian].
 17. Infografika dnia: u Zakhidnii Yevropi audytoriiia naibilshe doviriiae suspilnym movnykam [Infographics of the day: in Western Europe, the audience trusts social broadcasters most]. (June 19, 2018). ms.detector.media. Retrieved from https://ms.detector.media/mediaprovsvita/research/infografika_dnya_u_zakhidniy_evropi_audytoryia_naybilshe_doviryae_suspilnim_movnykam/ [in Ukrainian].
 18. *Denysenko L.* (March 5, 2019). Yaki zakonoproekty mozhut dozvolity pravookhorontsiam diznavatysia, shcho vy chytaiete, dyvytesia ta pyshete [What laws can allow law enforcement officers to know what you read, watch and write]. detector.media. Retrieved from <https://detector.media/withoutsection/article/163840/2019-03-05-yaki-zakonoproekty-mozhut-dozvoliti-pravookhorontsyam-diznavatysia-shcho-vi-chytaete-divitesyata-pishete/> [in Ukrainian].
 19. Dohovory ta konventsii Rady Yevropy, ratyfikovani Ukrainoiu [Agreements and conventions of the Council of Europe, ratified by Ukraine]. (n.d.). www.coe.int. Retrieved from <http://www.coe.int/ru/web/conventions/search-on-states/-/conventions/treaty/country/U> [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Пилипчук В., Дзьобань О.* Глобальні виклики й загрози національній безпеці в інформаційній сфері [Електронний ресурс] // Вісн. Нац. академії правових наук України // К. — № 3 (78). — 2014. — Режим доступу: http://nbuv.gov.ua/UJRN/varny_2014_3_6

2. Указ президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України” [Електронний ресурс] // 25.02.2017. — Режим доступу: <https://www.president.gov.ua/documents/472017-21374>
3. *Lerche Ch., A, Said.* Politics Concepts of International in Global Perspective / Ch. Lerche, A, Said. — USA, 1979. — 336 p.
4. *Вебер М.* Избранное. Образ общества: пер. с нем. / М. Вебер. — М.: Юристъ, 1994. — 704 с.
5. *Гогвуд Б., Іан Л.* Аналіз політики для реального світу / пер. з англ. А. Олійник, наук. ред. пер. В. Тертичка. — К.: Вид-во Соломії Павличко “Основи”, 2004. — 396 с.
6. *Горбуїн В., Качинський А.* Засади національної безпеки України. — К.: Інтер-технологія, 2009. — 272 с.
7. *Конах В., Лазоренко О.* Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації [Електронний ресурс] / В. К. Конах, О. А. Лазоренко // Стратегічні пріоритети. — 2014. — № 2. — С. 73–78. — Режим доступу: http://nbuv.gov.ua/UJRN/sra_2014_2_13
8. *Roberts Al. S.* Entangling Alliances: Nato’s security of information policy and the entrenchment of State Secrecy [Online tool]. — 2002. — Available at: https://www.researchgate.net/publication/228222455_Entangling_Alliances_NATO’s_Security_Policy_and_the_Entrenchment_of_State_Secrecy
9. *Cornish P.* Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. — Brussels: European Parliament. — 2014. — 24 p.
10. National Strategy for Switzerland’s protection against cyber risks [Online tool]. — 2012. — Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf
11. 2018 reform of EU data protection rules [Online tool]. — 2016. — https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
12. *Почепцов Г.* Світ базується на інформації та будується нею [Електронний ресурс] // Інтернет-видання // Київ: Детектор медіа. — 04.02.2019. — Режим доступу: <https://detector.media/withoutsection/article/144566/2019-02-04-svit-bazuetsya-na-informatsiitabuduetsya-neyu/>
13. *Почепцов Г.* Как убить фейк, или где украинские контр-нарративы [Електронний ресурс] // Інтернет-видання // Київ: Хвиля. — 13.02.2019. — Режим доступу: <https://hvylya.net/analytics/society/kak-ubit-feyk-ili-gde-ukrainskie-kontr-narrativyi.html>
14. *Платоненко А.* Сучасні загрози інформаційної безпеки для державних та приватних установ України [Електронний ресурс] // Київ: Сучасний захист інформації. — 2015. — № 4. — 120 с. — Режим доступу: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/428>
15. *Olavsrud T.* 9 biggest information security threats through 2019 [Online tool]. — 2017. — Available at: <https://www.itworld.com/article/3185725/9-biggest-information-security-threats-through-2019.html>
16. *Мусієнко І. В.* Етнічний лобізм як інструмент нарощування “м’якої сили” України // “Гілея: науковий вісник”: зб. наук. пр. — К.: ВІР УАН. — 2013. — Вип. 77 (№ 10). — 352 с.
17. Інфографіка дня: у Західній Європі аудиторія найбільше дові-

- ряє суспільним мовникам [Online resource]. — 2018. — https://ms.detector.media/mediaprosvita/research/infografika_dnua_u_zakhidnyy_evropi_auditoriya_naybilshe_doviryae_suspilnim_movnikom/
18. Які законопроекти можуть дозволити правоохоронцям дізнаватися, що ви читаєте, дивитися та пишете [Електронний ресурс]. — 2019. — <https://detector.media/withoutsection/article/163840/2019-03-05-yaki-zakonoproekti-mozhut-dozvoliti-pravookhorontsyam-diznavatisya-shcho-vi-chitaete-divitesya-ta-pishete//>
19. Договори та конвенції Ради Європи, ратифіковані Україною [Електронний ресурс]. — Режим доступу: <http://www.coe.int/ru/web/conventions/search-on-states/-/conventions/treaty/country/U>