SOCIAL AND BEHAVIORAL SCIENCES

DOI https://doi.org/10.51647/kelm.2021.3.1.25

BEZPIECZEŃSTWO INFORMACJI NA UKRAINIE: CELE, ZADANIA, ZAGROŻENIA I WYZWANIA NA DRODZE DO SPEŁNIENIA ŚWIATOWYCH WYMAGAŃ

Olesia Antokhiv-Skolozdra
kandydat nauk politycznych,
docent Katedry Stosunków Międzynarodowych i Służby Dyplomatycznej
Wydziału Stosunków Międzynarodowych
Lwowskiego Uniwersytetu Narodowego imienia Iwana Franki
(Lwów, Ukraina)
ORCID ID: 0000-0003-4374-2541
e-mail: olesya.antokhiv@lnu.edu.ua

Adnotacja. W artykule zwrócono uwagę na badanie systemu bezpieczeństwa informacji współczesnego społeczeństwa ukraińskiego na drodze od stawania się do spełnienia światowych wymagań. W ramach analizy teoretycznej określono podejścia do celów, zadań i kluczowych elementów zapewnienia odpowiedniego bezpieczeństwa. Ustalono, że pojęcia „bezpieczeństwo międzynarodowe" i „bezpieczeństwo narodowe" są niepodzielne. Prześledzono próbę przestrzegania przez państwo standardów światowego systemu bezpieczeństwa i osiągnięcia poziomu krajów przywódczych od uzyskania niepodległości do czasów współczesnych.

Przeanalizowano kryteria przystąpienia społeczeństwa do globalnej społeczności informacyjnej na poziomie legislacyjnym i wykonawczym. Udowodniono, że celem systemu bezpieczeństwa jest ochrona w różnych obszarach działalności człowieka, od politycznych i międzynarodowych do prywatnych konsumentów produktów informacyjnych.

W artykule przedstawiono wyniki analizy potencjalnych zagrożeń i ich skutków dla społeczeństwa.

Szczególną uwagę zwrócono na kryteria współpracy ukraińskich odpowiednich instytucji z Unią Europejską i NATO. Należy zauważyć, że członkostwo w Unii Europejskiej i NATO są priorytetem dla Ukrainy.

Słowa kluczowe: bezpieczeństwo informacji, bezpieczeństwo narodowe, ochrona informacji, źródła informacji, zagrożenia informacyjne, Unia Europejska, NATO.

INFORMATION SECURITY IN UKRAINE: GOALS, TASKS, THREATS AND CHALLENGES ON THE WAY TO MEETING GLOBAL REQUIREMENTS

Olesya Antokhiv-Skolozdra
Candidate of Political Science,
Associate Professor at the Department of International Relations and Diplomacy
of the Faculty of International Relations
Ivan Franko National University of Lviv (Lviv, Ukraine)
ORCID ID: 0000-0003-4374-2541
e-mail: olesya.antokhiv@lnu.edu.ua

Abstract. The article is devoted to the research of Information Security System of modern Ukrainian society on its way from establishment to meeting global requirements. Within the systemic theoretical analysis approaches to the goals, tasks and key elements of providing the adequate security support are defined. It is also depicted that the concept of "information security" and "national security" are inseparable. The state's attempts to comply with the global security standards have been steadily increasing since the early age of a newly independence until current time, and yet show the determination to meet the demands of the world key leaders.

The criteria of society's entry into global information community are analyzed on the legislative and regulatory levels. It shows that the goals of the security system include protection in various sphere of human activities from political and international sphere to private consumption of information products. The paper represents the results of the analysis of potential threats and their consequences for the society.

Particular attention is paid to the criteria to meet by Ukrainian responsible agencies in terms of information security interaction with the European Union and NATO. It is determined that the EU and NATO memberships are on the priority list for today.

Key words: information security, national security, information protection, media sources, information threats, European Union, NATO.

ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ: ЦІЛІ, ЗАВДАННЯ, ЗАГРОЗИ ТА ВИКЛИКИ НА ШЛЯХУ ДО ВИКОНАННЯ СВІТОВИХ ВИМОГ

Олеся Антохів-Сколоздра
кандидат політичних наук,
доцент кафедри міжнародних відносин і дипломатичної служби
факультету міжнародних відносин
Львівського національного університету імені Івана Франка (Львів, Україна)
ORCID ID: 0000-0003-4374-2541
e-mail: olesya.antokhiv@lnu.edu.ua

Анотація. У статті приділено увагу дослідженню системи інформаційної безпеки сучасного українського суспільства на шляху від становлення до виконання світових вимог. У межах теоретичного аналізу визначено підходи щодо мети, завдань і ключових елементів забезпечення належної безпеки. Встановлено, що поняття «міжнародна безпека» та «національна безпека» є нероздільними. Простежено намагання держави дотримуватися стандартів світової системи безпеки та досягти рівня країн-лідерів від здобуття незалежності до сучасного періоду.

Проаналізовано критерії приєднання суспільства до глобальної інформаційної спільноти на законодавчому та виконавчому рівнях. Доведено, що метою системи безпеки є захист у різних сферах людської діяльності: від політичної та міжнародної до приватного споживача інформаційної продукції.

У статті наведено результати аналізу потенційних загроз та їхніх наслідків для суспільства.

Особливу увагу приділено критеріям співпраці українських відповідних установ з Європейським Союзом і НАТО. Наголошено, що членство в Європейському Союзі та НАТО є пріоритетним для України.

Ключові слова: інформаційна безпека, національна безпека, захист інформації, інформаційні джерела, інформаційні загрози, Європейський Союз, НАТО.

Introduction. Increasing globalization and radical transformation in civilization evolution at the turn of the millennia have resulted in emerging a fundamentally new format of the world order, when the main directions of development of countries are connected with the formation of a universal information space, which is the space of information vulnerability and national security of all countries.

The analysis of the content of modern threats to any state shows that both technologies of external and internal influence and technologies of ensuring national interests are inherently informational in nature.

Ensuring national security is one of the most important tasks of a state nowadays. Over time, the meaning of the concept of "national security", forms and methods of ensuring it have changed. The rapid development of information technology in the late twentieth century also led to an increase in the relative importance of certain aspects of national security. As a result of the information revolution, information resources are gradually becoming the main value for society in general and the individual in particular.

Organization of a society began to transform in the direction of re-distribution of real power from traditional structures to the centers of information flow management, increased the influence of the media. Informatization and computerization are radically changing the face of a society. In such circumstances, information security is gradually coming to the fore in the field of national security.

Research of various aspects of information security issue is presented in a number of scientific papers: establishment of information society as a new global formation was studied by D. Bell, E. Toffler, A. Bentley, B.J. Ney and W. Owens, T. Parsons, B. Buddy, K. Shannon, R.-J. Schwarzenberg. Among Ukrainian scholars, investigating national information security are O. Baranova, O. Solodka, A. Voitsikhovskyi, E. Makarenko, O. Dovhan, A. Barovska and others. However, despite the rapid grow in interest towards information security area and a sufficient number of publication, the topic of the researched issue stays one of the most significant in modern society.

The current research is aimed at covering several areas of principles such as formation and functioning of the state information policy in the context of globalization, as well as compliance with the normative requirements of the world key players in this sphere.

The main part. The national information space of Ukraine is a sphere in which the state acts as a guarantor of integrity on the following basis: a single state policy defined by laws binding on all participants in information activities, regardless of ownership; preservation of the state's ownership of the leading objects, its use of the appropriate sources for the implementation of regulatory influence on public relations in the field of information; economic support of targeted programs, implementation of appropriate protectionist measures (Horovyi).

At the legislative level, the key elements of the information space of Ukraine are the national information resources (including documents, results of intellectual, creative and information activity, databases and data banks, all types of archives, libraries, museum funds and others, containing data, information and knowledge) and Information infrastructure with its organizational and technological structures (ensuring formation, operation and development of the information space, as well as the collection, processing, storage, dissemination and efficient use of information resources), information and telecommunication structures (territorially distributed state and corporate computer networks, telecommunication networks and systems of special purpose and general use, networks and data transmission channels, means of management of information flows) and system of mass media (printed and electronic ones – TV, radio companies, news agencies, book publishing complexes, cinematographic, library, archival, etc.) (Oliynyk, 2014: 59).

The goals of information security policy include realization of the constitutional rights of citizens, society and the state to information; protection of information sovereignty of Ukraine, in particular, the national information resource, systems of formation of public consciousness; ensuring the level of information sufficiency for decision-making by state institutions, enterprises and individuals; proper membership of the country in the world information space (Konstytutsiia Ukrainy, Art. 34).

Among the tasks of the information security are identifying, assessing and predicting the behavior of sources of threats to information security, which is carried out by operative monitoring of an information situation; development, coordination and introduction of a unified state policy system and security in the field of national information as well as international information relations, particularly, in creating the image of the state (Stratehiia natsionalnoi bezpeky Ukrainy, 2015).

Nevertheless, protection of an individual in a state cannot be underestimated. Thus, creation of electronic files, where files are stored for the entire population of the country – is a reality. In the mid-90's in Ukraine, following the example of developed countries, each citizen began to be assigned a personal tax number – identification code.

In the modern world every intelligence agency holds index cards – databases for millions of people. In France alone, such information databases are available to five governmental agencies (European Union Agency for Network and Information). Therefore, the issue of personal information, has acquired a considerable importance, although solution to this problem is quite a complicated task.

Following the goals and objectives, it's worth highlighting the main areas of Information Security Policy, of which the top four are: ensuring information sufficiency for decision making, data protection, that is protection of information resources, monitoring the national information space (as systems of formation of mass consciousness formation) and presence in the global information space.

Let's consider these areas in more detail. Regarding the issue of information supply for decision-making John Foster Dulles wrote: "If someone doubts the importance of objective information, I would recommend to analyze mistakes made by the leaders of states, because they followed bad advice, misjudging actions or reactions of other countries" (Holsti, 1970: 132). Another important aspect is information sufficiency in determining the reliability of information sources. Approaches to facts interpretation are largely related to a system of guidelines, stereotypes and symbols of the analyst, therefore possibility of deliberate awareness-raising or propaganda campaigns against analysts and decision makers is not excluded (Jowett, 2018: 157).

Hereto, we also suggest the types of issues, Governmental Agencies mostly operate: natural sciences, healthcare, scientific personnel, applied sciences, geographical data, transport, communications, economic, military, sociological, political and personalities.

Under the current circumstances in political and economic decision-making process, analyzing collected information has become decisive. Today the main problem is not obtaining certain information, but its scrutinizing, that is, the separation of the so-called "noises" and the correct interpretation of the information. Thus, requirements to be met in this fields can be concentrated in such slogan: "Report timely, accurately, clearly" (Diesch, 2020).

Considering the situation that has developed in Ukraine with receiving and processing "international information", it's worth mentioning that the process of setting up its own system for providing information to the public authorities of the young country began immediately after independence.

The Committee on Information Policy of Ukraine and its constituents, relevant divisions of the Office of the National Security Council, Ministry of Foreign Affairs, Security Service, Ministry of Defense of Ukraine, State Committee for the Protection of the State Border were established. The activities of the Ukrainian special services in the field of intelligence are coordinated by the Intelligence Committee under the President of Ukraine, headed by the First Deputy Secretary of the National Security and Defence Council of Ukraine, V. Radchenko.

Ukraine's information and analytical environment is gradually developed. In 1992, the National Institute of Strategic Studies began its work, which is the Governmental Institution for Research, Analytical Forecasting and Strategic Planning in order to provide information to the National Security and Defense Council and the President of Ukraine. The relevant Institutes of the National Academy of Sciences of Ukraine conduct their scientific work. Independent information and analytical centers have been set up. However, the information and analytical environment in the Ukrainian independent state hasn't fully met the requirements of the time yet, still requiring a number of adjustment to independence of scientific and analytical institutions from political influences, formation of a professional community, etc. (Dovhan, 2013: 75).

Being aware of current challenges, the general system of information protection nowadays covers the following areas: legislative and regulatory, law enforcement and judicial protection; organizational and technical support measures aimed at preventing threats to the security of information resources; information risk insurance (Pro osnovy natsionalnoi bezpeky Ukrainy, 2003).

Maintaining the use and control of national resources is carried out in accordance with the state defense legislation. Moreover, the structure of national resources, their status and the procedure for registration and use are determined by the Cabinet of Ministers of Ukraine (Barovska, 2014).

In order to ensure the development of national resources, the main objectives include: ensuring access to resources, including foreign ones, through global information networks; legal regulation of social relations connected with the advancement, use and protection of national resources; issueing recommendations for bringing national resources into common standards on the basis of the latest information technologies, international standards, unified classification and coding systems; establishing effective national search, geo-information and navigation systems; promoting the national content on the information market (Solodka, 2015: 46).

Substantial part of a State Security along with contemporary challenges is awareness of obstacles and dangers. Experts of the Razumkov Center have identified the main threats to Ukraine's Information Security implementation and possible negative consequences.

Hense, the most alarming are restrictions on freedom of speech and access to information, violation of the regular mode of functioning of critical information networks, management systems, implementation of political censorship, in particular, censorship on Internet by expanding the powers of law enforcement agencies.

Although, the list of mentioned above threats is not complete, it may lead to unavoidable hazardous consequences, like closure of opposition media, violence against journalists, dissemination of biased and incomplete information, manipulation of public opinion by the state authorities, financial and political circles; negative influence of mass media on public consciousness, loss of public support from the community, disruption of the system of public authorities, leakage of secret, confidential and other information with limited access, significant losses of economic, political, military and other nature for the state, causing material and moral damage to individuals and legal entities, infringement of copyright, non-property rights and intellectual property rights; violation of democratic principles and norms of state activity, use of state mass media to influence the course and results of elections, aggravation of relations between branches of power, establishment of authoritarian political regime, negative attitude or even international isolation of Ukraine from the world community (Awan, 2017).

Fortunately, the system of information security and protection in Ukraine is quite well-developed. It is presented by a certain legal framework which consists of the Laws of Ukraine "On Information", "On Protection of Information in Automated Information Systems", "On State Secrets", etc. (Stratehiia kiberbezpeky Ukrainy, 2016). There is a wide range of Presidential Decrees and Resolutions of the Cabinet of Ministers of Ukraine regulating specific activities in the field of information protection, a licensing and certification system of activities, including production of goods and services in the field of technical and cryptographic protection of information (Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury). In the summer of 1998, the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine was established on the basis of the relevant units of the Security Service and the State Committee for Protection of State Secrets and Technical Information Protection, with the main task of ensuring the implementation of state policy in the field of cryptographic and technical protection of information. Positive changes also occur in production of national information security means, in particular in private sector of economy. Owing to the activity of the National Bank of Ukraine in the banking system, a high level of informatization has been achieved (Bilenchuk, 2018).

On the whole, in the Security System, the information potential is becoming increasingly important. This concerns the information intended for industrial and applied use, particularly in the military-industrial complex. However, the information that fills free time, influences the mood of the nation, the guidelines of its younger generation must also be taken into account. Such information is provided for society by the mass media, the other system of shaping mass consciousness (Boukes, 2020).

Along with the national information security tasks, another prerequisite for success in this sphere is coherence with the global demands. Thus, a necessary condition for the development of the information society in Ukraine is the integration of Ukraine into the European Union, which has been declared a priority of the country's foreign policy course. As noted, the processes of European integration are ensured by the implementation of "e-Europe" programs and for candidate countries – "Action Plan "e-Europe +", which became the basis for the implementation of strategic goals of the "Lisbon Strategy" (2000) (Communication from the Commission on Critical Information Infrastructure Protection).

The purpose of adaptation of the legislation of Ukraine to the legislation of the European Union is compliance of the legal system of Ukraine with the legal system of the European Union (acquis communautaire), which includes acts of the European Union legislation, adopted within the European Community, taking into account the criteria set by the EU for the countries that intend to join it (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions). Harmonization is in the adjustment of national legislation on the basis of the EU legal acts, in particular directives, which require domestic legislation to be brought into line with their provisions.

The main element of Ukraine's successful European integration is the achievement of a certain harmonization level of Ukrainian legislation with the EU legal norms. Approximation of Ukrainian legislation with the modern European legal system will ensure the development of political, business, social, cultural activity of Ukrainian citizens, as well as create the necessary preconditions for Ukraine to receive the status of a member of the EU. In addition, at the legislative level, Ukraine will adopt the best, proven in practice, experience of countries that have been successfully implementing state information policy for decades.

Harmonization of the information legislation of Ukraine with the European one should be carried out in the following directions:

− harmonization and implementation of the legislation of Ukraine on electronic digital signature and electronic document management in accordance with Directive 99/93 /EU of the European Parliament and of the Council of December 131999 on electronic signatures. It's worth mentioning that two laws have already been adopted in Ukraine on the basis of the European law model on electronic signature, the law "On electronic documents and electronic document management" and "On electronic digital signature" (Concerning measures for a high common level of security of network and information systems across the Union).

− adoption of legislation on e-commerce, taking into account the provisions of the model European law on e-commerce, which is recommended for adoption for all countries that intend to integrate into the European e-space.

− adjustment to legislation in the field of information security (on the protection of personal data), taking into account the Provisions of Recommendation No R (99) 5 of the Committee of Ministers to Member States of the Council of Europe on the Protection of Privacy on the Internet, which approved the Guidelines for the Protection of Individuals with regard to the Collection and Processing of Personal Data on Information Highways of February 23 1999, other recommendations of the Committee of Ministers and directives of the European Union (Council Framework Decision 2005/222/JHA on Attacks Against Information Systems).

− coordination with the EU legislation requires legal regulation of activities in the field of informatization, implementation and operation of e-government, copyright protection, law enforcement of intellectual property rights in network, consumer protection, domain name protection, advertising, trademark registration, liability for illegal use of ICT.

Information policy of Ukraine from the perspective of joining NATO. An essential aspect of protecting Ukraine's information space is the prospect of our country's accession to NATO (Soskin, 2008). Nowadays NATO has begun to deal with the issue of information security, having gained experience primarily from the Alliance member states. A great number of seminars and discussions on information risks, cyberterrorism, and protection of classified state information are held on permanent basis with the view to reaching success in maintaining the issue (NATO Industry Cyber Partnership).

Ukrainian information specialists are highly valued in the world labor market. A large number of computer specialists, engaged into prominent world companies, particularly, in the USA, testifies to the vast potential of Ukraine in the information sphere.

Regarding the thesis "what NATO can give to Ukraine and Ukraine to NATO" (Voitsikhovskyi, 2020), the answer is incredibly simple and straightforward: "Security has no borders". We have something to work on together. It cannot be claimed that information security is NATO's first and only priority, but it is an important aspect of the Alliance member states' overall security (Security Council. Resolution 2341, 2017).

To achieve compliance with NATO information security standards, it is necessary to accomplish the following regulations:

− formation and implementation of a unified state policy to ensure the protection of national interests from threats in the information sphere, coordination of state authorities to ensure information security and improve legislation in information security;

− improving information infrastructure, accelerating the development of new information technologies and their dissemination;

− establishing the necessary balance between the need for the free exchange of information and acceptable restrictions on its dissemination; development of electronic certification and cryptography systems, including staff training;

− unification of means of search, collection, storage, processing and analysis of information, taking into account Ukraine's entry into the global information infrastructure and compliance with world standards;

− development of the domestic industry of telecommunication and information resources, their priority, in comparison with foreign analogs, distribution in the domestic market, and also the acceleration of processes of modernization of material and technical base and maintenance of protection of information resources and protection of the state information resources and, first of all, in public authorities and at the enterprises of the defense complex;

− effective counteraction towards information expansion and attempts to use the national information space.

It's worth emphasizing that the requirements hereinafter set up the obligations for all NATO's member-stated, Ukraine not being an exception. Thus, in March 1997, the Agreement between the Parties to the North Atlantic Treaty on the Protection of Information was concluded (Yarovenko, 2020). In addition, the NATO Secret Service Manual requires a member country to establish a national designated authority, responsible for the security of confidential information, through which the NATO Security Service contacts with the country. Moreover, within NATO, the functions of the national information security authority are as follows: ensuring the security of NATO secret information in national authorities, military and civilian structures, both inside and outside the country; management of the creation (or liquidation) of the governing body and regime departments; conducting periodic inspections to verify compliance with NATO's rules on the protection of secret information in national organizations at all levels, both military and civilian; ensuring the loyalty of all persons – citizens of a given country, by the nature of their activities admitted to secret information, under the standards and rules of information protection of NATO; ensuring the development of information protection plans in emergencies, to prevent the loss of confidentiality of NATO secret information.

It can be stated that the system of protection of the national information space has been formed and operates in Ukraine. It includes, first of all, an extensive legal framework for the media, consisting of the Constitution of Ukraine and the relevant Laws of Ukraine ("On Information", "On Print Media (Press)", "On Television and Radio Broadcasting", "On the National Council on Television and Radio Broadcasting", "On News Agencies", "On Advertising", etc.), the National Council on Television and Radio Broadcasting, the State Committee on Information Policy and Television and Radio Broadcasting (Onyshchenko, 2014). There are also other executive bodies. However, the measures of the national information space protection do not yet fully meet the modern capabilities of the country.

Conclusions. The information policy of the state must be analyzed from the standpoint of the national information space. For information policy in the information space, relevant are those objects and processes that can be influenced by information policy tools and techniques to influence the decision-maker and society at large.

The level of development of the information space affects all spheres of activity of the individual, society, and civilization. This considerably complicates the process of forming and implementing the information policy of the state, as it is necessary to formalize the behavior of the dynamic system and its component base, which like the information space, exists only in dynamics.

On the one hand, development, creation, and implementation of a system of State Information Security Policy should take into account the technical-technological and human dimensions of civilization. On the other hand, accelerated implementation of national informatization programs is a strategic task of the state because the availability of information infrastructure will promote acquiring new knowledge.

The uncontrolled emergence of fundamentally new information spaces and medium for the circulation of information has brought the issue of the management of information processes, in fact, the problem of the state's information security, to the forefront of all domestic and foreign policies.

The Information Security System, seeking to counterbalance all the factors, should improve the system of coordination of decisions and actions both national and global levels.

Bibliography:

1. Баровська А.В. Інституційне забезпечення державної комунікативної політики: досвід країн Європи : аналітична доповідь. Київ : НІСД, 2014. 40 с.
2. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право»*. 2020. (29). С. 281–288. DOI: 10.26565/2075-1834-2020-29-38.
3. Вступ до НАТО – стратегічний вибір України / за заг. ред. О.І. Соскіна. Київ : Інститут трансформації суспільства, 2008. 192 с.
4. Горовий В.М. Правові перспективи національного розвитку [Електронний ресурс]. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1068:pravovi-perspektivi-natsionalnogo-rozvitku&catid=127&Itemid=460.
5. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика*. 2013. № 4 (40). С. 72–82.
6. Конституція України [Електронний ресурс]. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр.
7. Концепція створення державної системи захисту критичної інфраструктури [Електронний ресурс]. URL: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi.
8. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні. *Юридичний вісник*. 2014. № 2 (31). С. 59–65.
9. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища / О.С. Онищенко та ін. ; НАН України, Національна бібліотека України ім. В.І. Вернадського. Київ, 2014.
10. Правові засади інформаційної безпеки / П.Д. Біленчук та ін. ; за ред. П.Д. Біленчука. Харків, 2018. 289 с.
11. Про основи національної безпеки України : Закон України від 19 червня 2003 р. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351.
12. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. № 3 (15). С. 36–42.
13. Стратегія кібербезпеки України [Електронний ресурс]. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.
14. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 р. № 287/2015. URL: www.president.gov.ua.
15. Awan I. Cyber-Extremism: Isis and the Power of Social Media. *Society*. 2017. 54 (2). P. 138–149. DOI: 10.1007/s12115-017-0114-0.
16. Boukes M., Jones N.P., Vliegenthart R. Newsworthiness and story prominence: How the presence of news factors relates to upfront position and length of news stories. *Journalism*. 2020. 146488491989931. DOI: 10.1177/1464884919899313.
17. Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.
18. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and information security: proposal for a European policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
19. Concerning easures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
20. Council Framework Decision 2005/222/JHA on Attacks Against Information Systems. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
21. Diesch R., Pfaff M., Krcmar H. A comprehensive model of information security factors for decision-makers. *Computers & Security*. 2020. 92. 101747. DOI: 10.1016/j.cose.2020.101747.
22. European Union Agency for Network and Information. URL: https://www.enisa.europa.eu/about-enisa.
23. Holsti O. The "Operational Code" Approach to the Study of Political Leaders: John Foster Dulles' Philosophical and Instrumental Beliefs. *Canadian Journal of Political Science*. 1970. 3 (1). P. 123–157. DOI: 10.1017/s000842390002713x.
24. Jowett S., O'Donnell V. Propaganda & Persuasion. California : SAGE Publications. 2018. 416 p.
25. NATO Industry Cyber Partnership. URL: https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.
26. Security Council. Resolution 2341 (2017). Adopted by the Security Council at its 7882nd meeting, on 13 February 2017. URL: https://undocs.org/S/RES/2341(2017).
27. Yarovenko H., Kuzmenko O., Stumpo M. DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges*. 2020. 4 (3). P. 142–153. DOI: 10.21272/sec.4(3).142-153.2020.

References:

1. Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Society*, 54(2). P. 138–149. DOI: 10.1007/s12115-017-0114-0.
2. Barovska, A. (2014) Instytutsiine zabezpechennia derzhavnoi komunikatyvnoi polityky: dosvid krain Yevropy: analit. dop. [Institutional provision of state communication policy: experience of European countries: analytical report] K.: NISD [in Ukrainian].
3. Bilenchuk, P. (red.), Borysova, L., Neklonskyi, I., Sobyna, V. (2018). *Pravovi zasady informatsiinoi bezpeky* [Legal provisions of information security]. Kharkiv [in Ukrainian].
4. Boukes, M., Jones, N. P., & Vliegenthart, R. (2020). Newsworthiness and story prominence: How the presence of news factors relates to upfront position and length of news stories. *Journalism*, 146488491989931. DOI: 10.1177/1464884919899313.
5. Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.
6. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: proposal for a European policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.
7. Concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
8. Council Framework Decision 2005/222/JHA on Attacks Against Information Systems. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.
9. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92, 101747. DOI: 10.1016/j.cose.2020.101747.
10. Dovhan, O. (2013) Orhanizatsiia pravovoho harantuvannia bezpeky informatsiinykh obminiv u konteksti hlobalizatsii [Organization of Legal Guarantees of Informational Exchange in the Context of Globalization]. *Pravova informatyka*. 4(40). P. 72–82 [in Ukrainian].
11. European Union Agency for Network and Information. URL: https://www.enisa.europa.eu/about-enisa.
12. Holsti, O. (1970). The "Operational Code" Approach to the Study of Political Leaders: John Foster Dulles' Philosophical and Instrumental Beliefs. *Canadian Journal of Political Science*, 3(1). P. 123–157. DOI: 10.1017/s000842390002713x
13. Horovyi, V. Pravovi perspektyvy natsionalnoho rozvytku [Legal Prospects of National Development]. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1068:pravovi-perspektivi-natsionalnogo-rozvitku&catid=127&Itemid=460 [in Ukrainian].
14. Jowett, S., & O'Donnell, V. (2018). *Propaganda & Persuasion*. California: SAGE Publications. 416 p.
15. Konstytutsiia Ukrainy [Constitution of Ukraine]. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр [in Ukrainian].
16. Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury [Concept of Creating State System of Critical Infrastructure Protection]. URL: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi [in Ukrainian].
17. NATO Industry Cyber Partnership. URL: https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html
18. Oliynyk, O. (2014). Stan zabezpechennia informatsiinoi bezpeky v Ukraini [The State of Information Security in Ukraine]. *Yurydychnyi visnyk*. 2(31). 59–65 [in Ukrainian].
19. Onyshchenko, O., Horovyi, V., Popyk, V. et al. (2014). *Natsionalni informatsiini resursy yak intehratyvnyi chynnyk vitchyznianoho sotsiokulturnoho seredovyshcha* [National Informational Resources as an Integral Factor of National Socio-Cultural Environment]. NAN Ukrainy, Natsionalna bibliotekaka Ukrainy im. V.I. Vernadskoho. K. [in Ukrainian].
20. Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 19.06.03 r. *Vidomosti Verkhovnoi Rady Ukrainy* [On Basics of National Security of Ukraine: the Law of Ukraine from 19.06.03 News of Verkhovna Rada of Ukraine]. 2003. No 39. St. 351 [in Ukrainian]
21. Security Council. Resolution 2341 (2017). Adopted by the Security Council at its 7882nd meeting, on 13 February 2017. URL: https://undocs.org/S/RES/2341(2017).
22. Solodka, O. (2015). Priorytety udoskonalennia informatsiinoi bezpeky Ukrainy [Priorities of Improvements of Ukraine's Informational Security]. *Informatsiia i pravo*. 3(15). P. 36–42 [in Ukrainian].
23. Soskin, O. (red.), (2008). *Vstup do NATO – stratehichnyi vybir Ukrainy* [Entering NATO – Strategic Choice of Ukraine]. K.: Instytut transformatsii suspilstva [in Ukrainian].
24. Stratehiia kiberbezpeky Ukrainy [Strategy of Cyber-Security of Ukraine]. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 [in Ukrainian].
25. Stratehiia natsionalnoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 26.05.15 r. No 287/2015. [Strategy of National Security of Ukraine: Presidential Decree from 26.05.15 No 287/2015]. URL: www.president.gov.ua [in Ukrainian].
26. Voitsikhovskyi, A. (2020). Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid) [Information Security as Component of National Security Systems (international and foreign experience)]. *The Journal of V. N. Karazin Kharkiv National University, Series "Law"*, 29). P. 281–288. DOI: 10.26565/2075-1834-2020-29-38 [in Ukrainian].
27. Yarovenko, H., Kuzmenko, O., & Stumpo, M. (2020). DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges*, 4(3), P. 142–153. DOI:10.21272/sec.4(3).