



ECONOMIC
AND TECHNICAL
ENGINEERING

Scientific and practical journal "Economics and technical engineering"

Vol. 1 No. 1 (2023)

Available since: 2023

Published: 2 times a year

Founders: State University of Economics and Technology

ISSN: 3041-1246

E-mail: etc@duet.edu.ua Journal homepage: <https://etc.org.ua>


JEL: D80, L98


DOI: 10.62911/etc.2023.01.01.03

Possibilities of adapting the EU experience in information security to the conditions of Ukraine

Citation:

Izmailov, Y., & Yegorova, I. (2023). Possibilities of adapting the eu experience in information security to the conditions of Ukraine. Scientific and practical journal "Economics and technical engineering", 1(1), 35–43. <https://doi.org/10.62911/etc.2023.01.01.03>

Yaroslav Izmailov
Prof. DSc, State Tax University, Irpin, Ukraine
e-mail: izmyar@ukr.net
 ORCID iD: 0000-0003-4853-205X

Iryna Yegorova
Assoc. Prof. PhD, State University of Economics and Technology, Kryvyi Rih, Ukraine
e-mail: yegorova_ig@duet.edu.ua
 ORCID iD: 0000-0002-7800-2810

Abstract: Information war, the promotion and spread of disinformation is a threat to regional, national and international security, especially in the conditions of rapid development of globalization, the fight against COVID-19, digitalization, increased international competition and pose new problems to the countries of the world. The Ukrainian-Russian war brought the information technologies of aggression and influence to a new level, therefore the experience of the developed countries of the European Union in information security is very relevant for Ukraine. Kremlin-controlled media outlets spread biased narratives, spread misinformation, and exploit existing vulnerabilities in Ukraine's media landscape. The purpose of the article is to determine the problems and prospects of ensuring the development of information security in Ukraine by adapting the positive experience of the countries of the European Union. Based on the analysis of the positive experience of the countries of the European Union, in order to ensure the information security of Ukraine, it is necessary to: pay great attention to the issues of cyber security, which is an organic part of information security; to rationally centralize powers in the field of information security; carry out active technological development and development of computer and information systems; to improve regulatory legal support and provisions of information security; to involve universities and employers in the professional training of information security specialists, to train the public in the form of information security courses; clearly define the main concepts and categories, make a list of relevant threats to information security; to provide truthful comprehensive information in combination with the dissemination of broad propaganda of national interests; take actions for the development of information culture and information society; to advertise the rules of information hygiene, prudence and legibility when contacting information; to educate Ukrainian citizens in critical thinking and the ability to recognize negative informational influence, manipulation, disinformation, falsification, etc.

Received: 10/09/2023

Accepted: 25/10/2023




Keywords: security, globalization, information, information security, foreign experience.

JEL: D80, L98

Possibilities of adapting the EU experience in information security to the conditions of Ukraine

Yaroslav Izmailov
Prof. DSc, State Tax University, Irpin, Ukraine
e-mail: izmyar@ukr.net
 ORCID iD: 0000-0003-4853-205X

Iryna Yegorova
Assoc. Prof. PhD, State University of Economics and Technology, Kryvyi Rih, Ukraine
e-mail: yegorova_ig@duet.edu.ua
 ORCID iD: 0000-0002-7800-2810

Abstract: Information war, the promotion and spread of disinformation is a threat to regional, national and international security, especially in the conditions of rapid development of globalization, the fight against COVID-19, digitalization, increased international competition and pose new problems to the countries of the world. The Ukrainian-Russian war brought the information technologies of aggression and influence to a new level, therefore the experience of the developed countries of the European Union in information security is very relevant for Ukraine. Kremlin-controlled media outlets spread biased narratives, spread misinformation, and exploit existing vulnerabilities in Ukraine's media landscape. The purpose of the article is to determine the problems and prospects of ensuring the development of information security in Ukraine by adapting the positive experience of the countries of the European Union. Based on the analysis of the positive experience of the countries of the European Union, in order to ensure the information security of Ukraine, it is necessary to: pay great attention to the issues of cyber security, which is an organic part of information security; to rationally centralize powers in the field of information security; carry out active technological development and development of computer and information systems; to improve regulatory legal support and provisions of information security; to involve universities and employers in the professional training of information security specialists, to train the public in the form of information security courses; clearly define the main concepts and categories, make a list of relevant threats to information security; to provide truthful comprehensive information in combination with the dissemination of broad propaganda of national interests; take actions for the development of information culture and information society; to advertise the rules of information hygiene, prudence and legibility when contacting information; to educate Ukrainian citizens in critical thinking and the ability to recognize negative informational influence, manipulation, disinformation, falsification, etc.

Keywords: security, globalization, information, information security, foreign experience.

Introduction

Today, information is a means of manipulating public and individual consciousness, as well as a weapon that, although virtual, is widely and successfully used in direct and hybrid confrontations, military conflicts.

Information war, promotion and spread of disinformation is a threat to national and international security, especially in the conditions of rapid development of globalization, fight against pandemic, digitalization, strengthening of international competition, military confrontation between countries. Wars in the information space create new challenges and threats to ensure the security of information interaction between the countries of the world.

Information warfare has become an integral part of modern conflicts, as states and non-state actors strategically use information to shape narratives, influence public opinion, and undermine the

security and stability of target countries. The Russian-Ukrainian information war creates significant challenges and threats to the information security of the European Union (EU). The main challenges facing the EU are the relentless disinformation campaigns spread by the Russian Federation to discredit Ukraine and its allies and the European Union itself. These campaigns are aimed at distorting information, manipulating public opinion and creating division in EU member states. By spreading false narratives and conspiracy theories, Russia seeks to sow discord and weaken European unity by influencing EU policy and decision-making processes.

The Russian-Ukrainian war brought the information technologies of aggression and influence to a new level. Therefore, the experience of the developed countries of the European Union in information security is very relevant for Ukraine. Kremlin-controlled media outlets spread biased narratives, spread misinformation, and exploit existing vulnerabilities in Ukraine's media landscape. The use of social media platforms to spread propaganda, manipulate public opinion, and incite online extremism poses a serious threat to Ukraine's information security. Therefore, it is important to consider the possibility of adapting the EU experience in information security to the conditions of Ukraine.

Materials and Methods

In the course of the research, the following methods were used: dialectical, generalization, comparison, system analysis, observation of economic activity, graphic, etc.

Results

The analysis of literary sources allows us to state that more and more attention is paid to the problems and prospects of the development of global, international and regional information security. At the same time, the definition of the vector of development and strategic tasks of ensuring Ukraine's information security in wartime conditions and in the period of the country's postwar revival requires a deep comprehensive analysis of the experience accumulated by the countries of the world in the security sphere and an assessment of the possibilities and expediency of its use in modern realities and in the future.

Among the modern methods of ensuring information security, the most important are: software-technical, managerial, technological, network and procedural, which allow to assess the level of compliance with information security and suggest directions for strengthening the protection of the information field of countries.

The purpose of the article is to determine the problems and prospects of ensuring the development of information security in Ukraine by adapting the positive experience of the countries of the European Union.

Article 17 of the Constitution of Ukraine (Constitution of Ukraine, 1996) states that ensuring information security is the most important function of the state and the business of the entire Ukrainian people.

Scientists define information security as (Zakharenko, 2019): 1. A type of national security aimed at ensuring human rights and freedoms regarding free access to information, creation and implementation of safe information technologies, and protection of property rights of all participants in information activities; 2. Practical activities aimed at preventing unauthorized access, application, detection and transformation of data.

Internal and external information threats can harm national and international relations, specific citizens.

Countering the informational threat will be a complex of socio-economic, organizational-management and normative-legal measures aimed at transforming the adverse impact of the threat. Given the nature of the threat, transformation will involve overcoming an existing or preventing a potential information threat, and depending on whether there is a possibility of complete neutralization of the threat, countermeasures will involve minimization (partial neutralization) or

elimination (full neutralization) of the impact of the information threat. The result of overcoming existing or preventing potentially possible information threats is the protection of national interests and ensuring the information sovereignty of the state (Fig. 1).

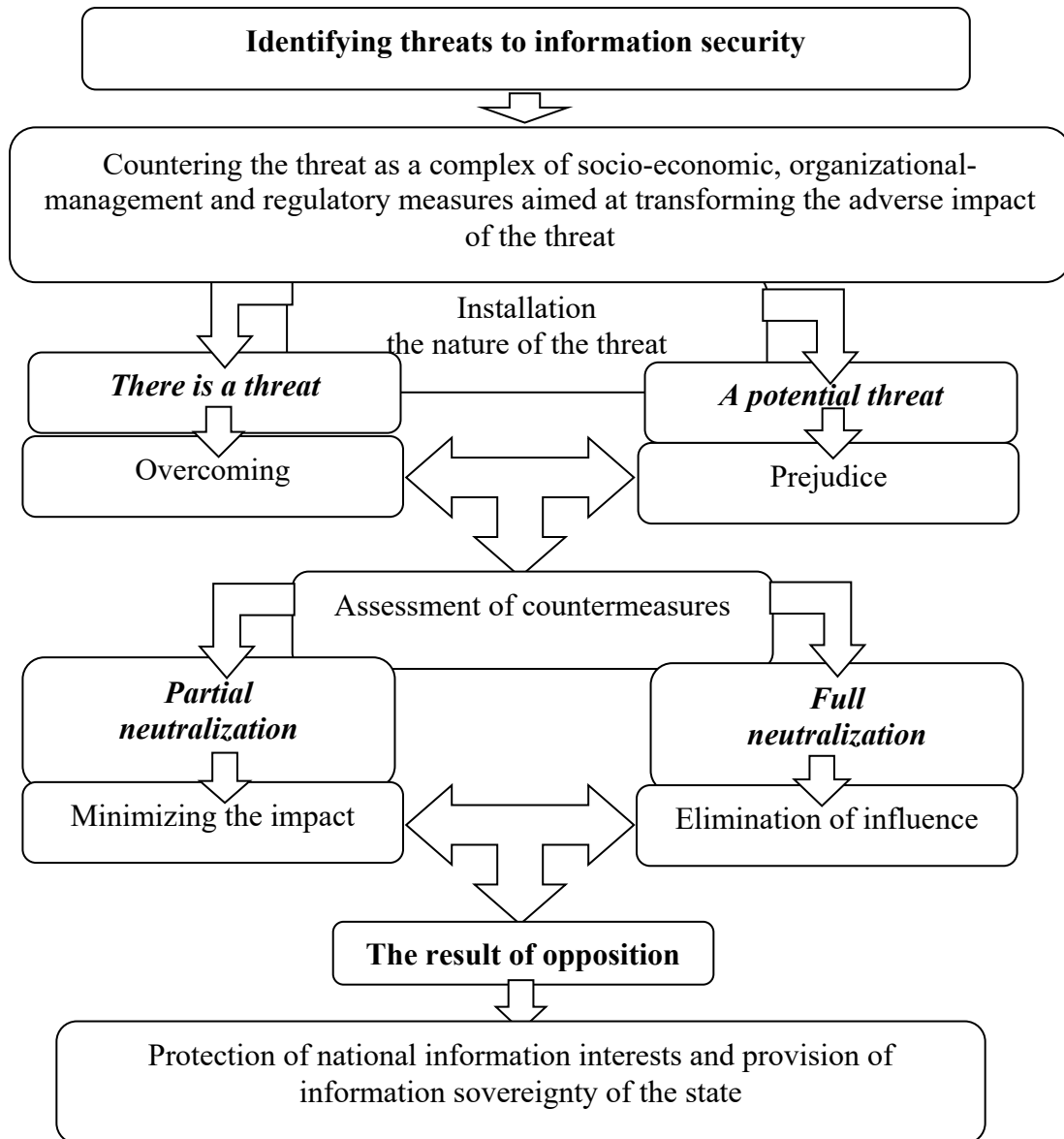


Figure 1. Algorithm for neutralization of threats to information security of the state

The Information Security Doctrine of Ukraine established the status of information security as an integral component of each of the spheres of national security. According to the doctrine of information security of Ukraine, which is set forth in the Law of Ukraine "On the National Informatization Program" (On the National Informatization Program, 2022), current threats to the national interests and national security of Ukraine in the information sphere are presented in fig. 2.

The doctrine became the basis for the formation of state policy in the field of information security of Ukraine, the development of projects of concepts, strategies, target programs and action plans for ensuring the information security of Ukraine, the preparation of proposals for further systematic improvement of the legal, methodical, scientific, technical and organizational provision of information security of Ukraine.

The CIA triad (confidentiality, integrity, availability) as a fundamental concept of information security in the EU contributes to the effective protection of information and data.

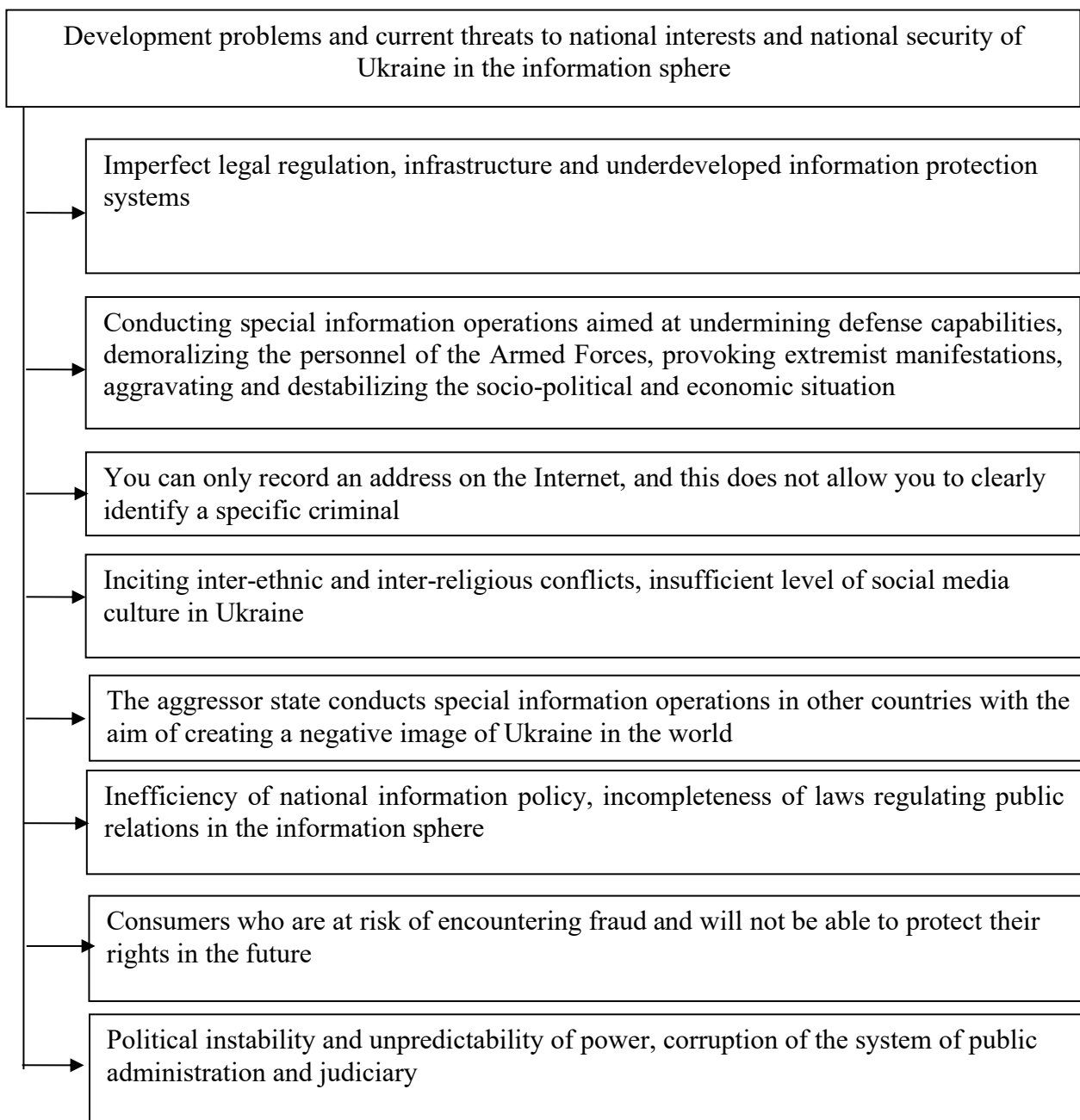


Figure 2. The main problems of development and threats to the national security of Ukraine in the information sphere

Privacy refers to the protection of confidential information from unauthorized access or disclosure. The EU information security policy prioritizes the privacy of personal data, intellectual property and classified information.

As technology continues to evolve, information security remains a critical issue for the European Union. By prioritizing confidentiality, integrity and accessibility, as well as ensuring the implementation of a comprehensive legal framework, risk management practices, incident response coordination, international cooperation initiatives and cyber security awareness, the EU is working to strengthen the protection of its information.

Another main pillar of the EU's information security policy is the Network and Information Security (NIS) Directive, which is the first pan-European legislation on cyber security. The NIS Directive aims to achieve a high overall level of cybersecurity in Member States by requiring them to adopt national strategies and capabilities, designate competent authorities and single points of

contact, cooperate and exchange information at EU level, and ensure that operators of essential services and providers digital services took appropriate security measures and reported incidents.

In January 2023, the NIS Directive (Proposal for directive on measures for high common level of cybersecurity across the Union, 2023) was replaced by the NIS2 Directive, which introduced stricter requirements and broadened the scope to cover more sectors and organizations vital to the EU economy and society. The NIS2 directive also addressed supply chain security, streamlined reporting obligations and harmonized sanctions across the EU. Member States have until October 2024 to transpose the NIS2 Directive into their national laws.

The EU is also investing in research and innovation to strengthen its information security capacity and strategic autonomy. As part of the Digital Europe program for the period 2021-2027 (Integration of Ukraine into the single digital market of the European Union: challenges, opportunities and obstacles, 2023), the EU has committed to invest €1.6 billion in cybersecurity capacity and the widespread deployment of cybersecurity infrastructure and tools in the EU for public administrations, businesses and individuals. The EU also supports the development of a European network of competences in the field of cyber security and a center for the coordination of research and innovation activities, the pooling of experience and resources, and the provision of advice on cyber security policy.

Using the example of evaluating the operation of the system in certain countries of the European Union, namely Germany and Poland, it can be concluded that in order to achieve the goal of ensuring information security in any sphere of public life, a clear and coordinated functioning of the subject of ensuring such security, which is exclusively vested specialized powers. It is the specialized body that can most effectively comply with the provision of information security, since it carries out the accumulation of special experience, improvement of the educational, technical, material, practical base, as well as baggage from interaction with other subjects of legal relations in the state and subjects of international law.

Using the example of Germany, it can be clearly determined that the proper basis for the further effective functioning of the legal mechanism for ensuring information security in the state is, first of all, effective and high-quality legal regulation (Kilimnik, 2023). One of the most important trends that should be borrowed from Poland in the context of ensuring information security is the active involvement of non-state actors, primarily members of civil society, in all processes.

The NATO Doctrine describes the concept of strategic communications in detail (Cards: what is strategic communication and who needs it, 2023). This concept covers the coordinated and effective use of NATO's various means of communication. Among them are public diplomacy, public relations, activities of the PR service of the armed forces, information and psychological operations, which are used to support the policy of the Alliance and implement measures aimed at achieving NATO's goals.

It makes sense for Ukraine to continue strengthening international cooperation with organizations such as NATO, OSCE, EU and UN in all spheres (Chitak, 2023). If possible, Ukraine should defend its positions and interests at international negotiations, in cooperation formats and in international courts. It is also necessary to actively use European and international standards in the field of cyber security, to develop the work of special bodies that are able to effectively interact with the relevant EU and NATO bodies, to involve Ukraine in joint exercises and trainings, where there is direct communication with experienced foreign specialists. The use of information technologies in the military sphere has opened up new opportunities for ensuring the defense capability of the state against an aggressor. The possession of information resources and their protection have become as important as the availability of weapons, ammunition, transport, etc. Only the advantage of Ukraine in the information confrontation with the Russian Federation will help to achieve the strategic goals of the country and the most desired result - victory.

Germany is one of the countries that actively uses the advantages of the private sector in the process of providing state departments. Thus, the "Hercules" program is the largest joint project of the public and private sectors in Europe ("Public-Private Partnerships"). The implementation of the program is provided for in the framework of the relevant contract between the Federal Department for the Development and Procurement of Weapons of the Bundeswehr and the joint venture

"Information-technik GmbH". The purpose of the latter is the implementation of the latest technologies, in particular in the field of ensuring information security, in the activities of the German Ministry of Defense and the Armed Forces. In general, a great deal of attention was paid to the innovative provision of the activities of the Ministry of Defense of the Federal Republic of Germany and the Armed Forces of this country. New information systems and communication technologies are constantly being implemented in this sector, and software for their protection is being developed.

Thus, in the above-mentioned country, it is necessary to ascertain the existence of a serious approach of the state leadership to ensuring the information security of employees of the defense sector, in particular, military personnel of the Armed Forces.

Therefore, the implementation of the process of ensuring national information security requires careful research and actualization of threats that arise in the external and internal environment, and lead to the weakening of state sovereignty and the impossibility of worthy defense of national economic interests in the conditions of war with the Russian Federation. Exogenous determinants have a particularly significant impact on information security, because due to their external influence, they are uncontrollable, unpredictable and unmanageable. A key task in the context of effective provision of information security of the state is the timely identification of information threats in order to minimize threats and use opportunities to eliminate them.

The development of highly intellectual, interesting and patriotic content is possible in the event of the implementation of measures for the systematic combination of science and the media through state support for the implementation and commercialization of the results of this activity. Also, the creation of powerful information content requires the state to implement and monitor the implementation of programs related to the development of scientific and technical activities and information security, to take measures regarding the international integration of science, media resources and education, to form a mechanism for coordinating scientific, technical and information activities, to provide assistance in the promotion of information, which will ensure countermeasures against external and subversive internal informational influence on Ukraine. The state information policy for ensuring the effectiveness of information security during war should be formed in compliance with the principle of multi-level protection and be based on coordinated actions and fruitful cooperation of business, mass media, state authorities, local self-government and civil society. Such concerted activity is the key to the effectiveness of information policy in wartime conditions. Based on the experience of the countries of the European Union, in order to ensure the information security of Ukraine, it is necessary to: 1. Clearly identify destabilizing factors and threats to information security; 2. Carry out a thorough analysis of information threats; 3. System monitoring of exogenous and endogenous information space; 4. Create an effective plan to counteract external information influences on the population by creating an effective system for implementing information policy mechanisms to identify and neutralize threats to Ukraine's national interests and national security in the information sphere, as well as to satisfy Ukraine's national interests in all spheres of the state's life; 5. Develop an effective system for protecting critical infrastructure objects from cyberattacks.

Conclusions

The current priority of the state management of information security of Ukraine is the institutionalization of this process based on the experience of the countries of the European Union, which should take place in such key areas as the development of the legal and methodological framework for ensuring the information security of the state in the direction of creating a single legislative space for the regulation of this process, as well as improving the interaction of state management bodies and institutions in the field of ensuring the information security of the state through a systematic and rational distribution of functions related to the implementation of this process.

The analysis of foreign experience made it possible to highlight the peculiarities of building an information policy and different approaches to ensuring information security of Ukraine. Based on

the experience of the countries of the European Union, in order to ensure the information security of Ukraine, it is necessary to:

- pay great attention to issues of cyber security, which is an organic part of information security;
- it is more rational to centralize powers in the field of information security;
- to carry out active technological development and development of computer and information systems;
- improve regulatory and legal provision of information security;
- to involve universities and employers in the professional training of information security specialists, to train the population in the form of information security courses;
- clearly define the main concepts and categories, make a list of relevant threats to information security;
- to provide truthful comprehensive information in combination with the dissemination of broad propaganda of national interests;
- take actions for the development of information culture and information society;
- advertise the rules of information hygiene, prudence and legibility when contacting information;
- to educate citizens of Ukraine in critical thinking and the ability to recognize negative informational influence, manipulation, disinformation, falsification, etc.

The presented problems and ways of improving international and regional information security based on the experience of the countries of the European Union will provide an opportunity to improve the security component and information hygiene of life in Ukraine.

It is advisable to focus further scientific research on the implementation of foreign experience of various countries for the development of information security mechanisms of Ukraine.

Conflicts of interest

The authors declare no conflict of interest.

Funding

This research received no external funding

Authors contribution

Conceptualization, Y.I. and I.Y.; methodology, Y.I.; software, Y.I.; check, Y.I., I.Y.; formal analysis, I.Y.; resources, I.Y.; analytical data, Y.I.; visualization, I.Y.; supervision, I.Y.; project administration, Y.I. All authors have read and approved the published version of the manuscript.

References

- Cards: what is strategic communication and who needs it (2023). *Center for Policy Consulting*. <https://cpc.com.ua/articles/kartki-scho-take-strategichna-komunikaciya-i-komuvona-potribna>
- Chitak, V., & Usmanov, Y. (2023). International and national legal analysis of the state of information security of Ukraine in conditions of armed conflict. *Scientific Bulletin of the Uzhhorod National University*, 2(76), 271–277. DOI <https://doi.org/10.24144/2307-3322.2022.76.2.43>
- Constitution of Ukraine (1996). Law of Ukraine dated 28.06.1996. Official website of the Verkhovna Rada of Ukraine. <https://zakon.rada.gov.ua/laws/show/254k/96-bp>
- Decree of the President of Ukraine dated December 28, 2021 No. 685 "On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy". <https://zakon.rada.gov.ua/laws/show/685/2021#n7>
- Integration of Ukraine into the single digital market of the European Union: challenges, opportunities and obstacles. *Official site EU-Ukraine Civil Society Platform*. <http://eu-ua-csp.org.ua>

- Kilimnik, I. (2023). Information society and information security. New challenges and new ways to overcome the information threats. *Scientific Bulletin of the Uzhhorod National University*, 2(76), 53–57. <https://doi.org/10.24144/2307-3322.2022.76.2.8>
- Law of Ukraine "On the National Informatization Program". No. 2807-IX (2022). <https://zakon.rada.gov.ua/laws/show/74/98-vr>
- Nishchymenko, O. (2016). Information security of Ukraine at the current stage of development of the state and society. *Our law*, (1), 17–23.
- On the decision of the National Security and Defense Council of Ukraine dated December 30, 2021 "On the Strategy for Ensuring State Security": Decree of the President of Ukraine dated February 16, 2022 No. 56/2022. Official website of the President of Ukraine. <https://www.president.gov.ua/documents/562022-41377>
- On the national security of Ukraine (2018). Law of Ukraine dated June 21, 2018 No. 2469-VIII. *Official website of the Verkhovna Rada of Ukraine*. <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
- Proposal for directive on measures for high common level of cybersecurity across the Union (2023). The Commission has adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). *Site European Commission*. <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
- Vyzdryk, V., & Melnyk, O. (2023). Information security in Ukraine: current state. *International scientific journal "Grail of Science"*, 24, 196–202. <https://doi.org/10.36074/grail-of-science.17.02.2023.034>
- Zakharenko, K. V. (2019). INTERNATIONAL EXPERIENCE IN INFORMATION SECURITY. *Modern Society: Political Sciences, Sociological Sciences, Cultural Sciences*. <https://doi.org/10.34142/24130060.2019.17.1.09>