DOI: https://doi.org/10.34069/AI/2022.54.06.16

How to Cite:
Chernysh, R., Prozorov, A., Tytarenko, Y., Matsiuk, V., & Lebedev, O. (2022). Legal and organizational aspects of destructive information impact counteracting: the experience of Ukraine and the European Union. *Amazonia Investiga*, *11*(54), 169-177. https://doi.org/10.34069/AI/2022.54.06.16

Legal and organizational aspects of destructive information impact counteracting: the experience of Ukraine and the European Union

Правові та організаційні аспекти протидії деструктивному інформаційному впливу: досвід України та Європейського Союзу

Received: May 16, 2022 Accepted: June 30, 2022

Written by:
Roman Chernysh[67]
https://orcid.org/0000-0003-4176-7569
Web of Science researcher code: AAV-4639-2020
Andrii Prozorov[68]
https://orcid.org/0000-0002-0905-7076
Web of Science researcher code: AAP-2986-2021
Yaroslav Tytarenko[69]
https://orcid.org/0000-0002-3062-5664
Vitalii Matsiuk[70]
https://orcid.org/0000-0002-5416-5463
Olexander Lebedev[71]
https://orcid.org/0000-0001-7112-2804

Abstract

With the functioning of the global Internet, the geopolitical struggle between the states has intensified significantly in the information sphere. Transformations of the security space in modern conditions are leading to extraordinary events in cyberspace in Europe and other countries, which are becoming more frequent and large-scale. This situation requires intensification of international cooperation in the field of information space protection.

A significant part of the risks in the information sphere arises due to the «lag» of legal regulation from scientific and technological progress. This has led to problems of protection of personal data of citizens and ensuring the sustainable operation of information and telecommunications systems of critical infrastructure. One of the main ways to overcome the «lag» is timely and proper regulation of these processes.

Effective international cooperation to protect the information space will be facilitated by:

Анотація

За умови функціонування глобальної мережі Інтернет геополітична боротьба між державами суттєво активізувалася в інформаційній сфері. Трансформації безпекового простору в сучасних умовах призводять до надзвичайних подій у кіберпросторі в європейських та інших країнах, які стають все частішими і масштабнішими. Така ситуація потребує активізації міжнародної співпраці у сфері захисту інформаційного простору.

Значна частина ризиків в інформаційній сфері виникає через «відставання» нормативно-правового регулювання від науково-технічного прогресу. Зазначене зумовило появу проблем захисту персональних даних громадян та забезпечення сталого функціонування інформаційно-телекомунікаційних систем критичної інфраструктури. Одним із основних шляхів подолання «відставання» є своєчасне і належне нормативно-правове регулювання вказаних процесів.

[67] Ph.D (Law), Associate Professor of the Department of Science of Law, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[68] Ph.D (Law), Associate Professor of the Department «Organizations of information security with limited access» of the National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[69] Ph.D (Law), National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[70] Ph.D (Law), Deputy director of Institute of Information Security of the National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[71] Ph.D (Law), Associate Professor, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.

improving coordination of actions and cooperation within international organizations in order to strengthen cyber resilience; purposeful fight against cybercrime in Ukraine and the world; development of cybersecurity dialogue at the national and international levels; close public-private partnership in the institutional provision of information and cybersecurity management.

Key words: destructive information impact, psychological impact, information security, Internet, critical infrastructure.

У контексті побудови ефективної системи протидії деструктивному інформаційному впливу актуальною проблематикою є вдосконалення форм і методів захисту інформації, критичної інформаційної інфраструктури та забезпечення інформаційно-психологічної безпеки громадян.
Дієвій міжнародній співпраці для захисту інформаційного простору сприятимуть: удосконалення координації дій та співробітництва у рамках міжнародних організацій з метою посилення кіберстійкості; цілеспрямована боротьба з кіберзлочинністю в Україні та світі; розвиток діалогу з кібербезпеки на національному та міжнародному рівнях; тісне державно-приватне партнерство при інституційному забезпеченні управління інформаційною та кібербезпекою.

Ключові слова: деструктивний інформаційний вплив, психологічний вплив, інформаційна безпека, мережа Інтернет, критична інфраструктура.

Introduction

With the functioning of the global Internet, the geopolitical struggle between states and other actors (law enforcement agencies, special services, officials of international organized crime groups, etc.) has significantly intensified in the information sphere. This is due to the ability to influence large, diverse and physically difficult to reach audiences using relatively small resources.

Forecasts of the development of the international security environment give grounds to believe that the subjects of national security need to take urgent precautionary measures to protect the interests of Ukraine in the information space as a whole, an essential component of which is cyberspace (Pohoretskyi, Cherniak, Serhieieva, Chernysh, & Toporetska, 2022).

It should also be noted that the transformation of security space in modern conditions is leading to extraordinary events in cyberspace, which are becoming more frequent and large-scale.

Currently, a significant part of the risks in the information sphere arises due to the «lag» of legal regulation from scientific and technological progress. In particular, in recent years there has been a powerful technological revolution in the use of computers and telecommunications, which has led to a significant increase in the use of PCs. This has led to problems with the protection of personal data of citizens and ensuring the sustainable operation of information and telecommunications systems of critical infrastructure.

One of the main ways to overcome the «backlog» is the timely and proper regulatory support of these processes. At the same time, our analysis of law enforcement practices to ensure information security as a component of national security in the European Union, gives reason to believe that a unified model of building an international security system is absent (Onyshchuk, Onyshchuk, Petroye & Chernysh, 2020; Vlasenko, Chernysh, Dergach, Lobunets & Kurylo, 2020; Chernysh, Pogrebnaya, Montrin, Koval, & Paramonova, 2020; Chernysh & Osichnyuk, 2021).

Given the need to build an effective system to combat destructive information impact, the issue of improving the forms and methods of information protection, critical information infrastructure and information and psychological security of citizens by all European countries is relevant (Tkachuk, 2017).

Materials and methods

In accordance with the purpose of the article, a number of scientific methods of modern epistemology were used in the process of scientific research. The methodological basis of the study was the theory of knowledge of legal phenomena as conceptual provisions, which were developed by prominent experts in the field of information law. In addition, special research methods were used, in particular: comparative - to compare the provisions of current Ukrainian legislation in the field of information security and regulations of the European Union; special legal - for a thorough analysis of regulations governing the procedure for combating destructive information influence; systematic approach and logical-legal method - to analyze the impact of negative factors on the constituent elements of the studied phenomenon and the formation of logical and specific theoretical and applied conclusions.

Results and discussion

According to today's realities, destructive informational influence on the Internet is carried out within the framework of special information operations, during which information resources are comprehensively used using traditional communication channels (television, radio, print, visual aids, etc.) and electronic (from news and entertainment to scientific and professional Internet resources, social networks).

The essence of measures of information influence on the Internet is the organized deliberate dissemination of false or biased messages on a large scale to achieve the political goals of states that carry out information expansion. Despite the fact that such events actually take place in cyberspace, they have very real consequences: interference in public administration processes, destabilization of critical infrastructure, increasing social tensions, exacerbation of interethnic and interfaith conflicts, diversification of public opinion and more.

Destructive information activities on the Internet are mostly hidden. This is due to the efforts to keep secret the interest and involvement of the initiating entity in their conduct.

In our opinion, it is possible to identify the following measures of information impact:

- propaganda (dissemination of certain ideas to form their support to selected target groups),
- disinformation (misleading, providing false, biased information);
- manipulative (the implementation of covert information and psychological influence on the audience in order to change its attitude to certain problems and programming behavior to support or perceive ideas that are beneficial to the initiator of information influence);
- diversifying (creating and giving false importance to small issues, focusing on them special and increased attention, distraction from real problems that require urgent, urgent solution);
- compromising (objects are public authorities and officials, individual actions or in general the policy of the top leadership of the state, which are presented in a negative, unfavorable light for them);
- destabilizing (destabilization of the socio-political or economic situation in the victim state, exacerbation of interethnic, interfaith conflicts, etc.).

An analysis of the statistics of law enforcement agencies and special services of a number of countries shows that in today's world no state is able to effectively combat cyber attacks and destructive influences in the information sphere.

In view of the above, Ukraine systematically organizes cooperation with international partners to protect national sovereignty in various spheres of public life. In the first round of the Ukraine-European Union Cyber Dialogue, held in June 2021, the parties agreed on the need to uphold the rule of law to ensure global, open, stable and secure cyberspace.

The parties exchanged information on the institutional structure and powers of bodies in the field of cyberspace, the latest developments in the development of legislative initiatives, including updates of EU Directive 2016/1148 on measures to ensure a high overall level of security of network and information systems across the Union (Directive (EU) 2016/1148, 2016).

Ukraine and the EU reaffirmed the importance of the Budapest Convention (Law No 2824-IV, 2001), which contributes to the improvement of national legislation and deepens international cooperation in the fight against cybercrime, both internationally and regionally. Ukraine has announced draft legislation amending the

Criminal Procedure and Administrative Codes of Ukraine. Both projects have been approved by the relevant committee of the Ukrainian Parliament and are awaiting approval (Ministry of Foreign Affairs of Ukraine, 2021).

The next step for Ukraine should be to develop national legislation taking into account the provisions of the updated EU strategy in the field of cyber security in the context of digital modernization in the coming years, approved by the Council of the European Union in March 2021.

This strategy was presented by the European Commission and the EU High Representative in December 2020. It contains the framework conditions for EU action to protect EU citizens and businesses from cyber threats, to develop a secure information system and to protect global, open, free and secure cyberspace.

According to the document, cybersecurity is a key factor in building a sustainable, green and digital Europe, as well as in achieving the EU's strategic autonomy, while maintaining an open European community economy.

The EU Council has identified key areas for cyber security in the coming years. Among them, in particular, the intention to create a network of operational centers for security throughout the EU, the main purpose of which will be forecasting, timely detection and response to cyber attacks on communications networks. At the same time, the EU must define an operational structure that will take care of coordination and crisis management to combat cyber attacks and threats.

A special place in the strategy is given to the rapid completion of the formation of the 5G communication network in the EU, its reliable protection and efforts to develop the next generation of communication systems.

It is also planned to raise security standards on the Internet, which remains an important tool for achieving the security goals of global communications. To achieve this goal, the EU will use the competitive advantages of its own industry, raise network security standards, including the use of modern systems of protection and encryption of information. Such protection will be provided primarily to law enforcement and judicial networks to ensure the effective exchange of operational information.

Cyber diplomacy will also be improved, providing EU tools to prevent and respond to cyber attacks if they are committed against the EU in areas such as the sustainability of supply networks, critical infrastructure and services, democratic procedures and the functioning of state institutions. economic security, etc.

Also, at the EU Intelligence and Situation Center (INTCEN) it is planned to create a special cyber intelligence group, which should strengthen the work of the agency in this area (Ministerio de Defensa de Espana, 2017).

In turn, Decree of the President of Ukraine № 447/2021 put into effect the decision of the National Security and Defense Council of Ukraine of May 14, 2021 on the Cyber Security Strategy of Ukraine.

The main subjects of cybersecurity were involved in its preparation: the Security Service of Ukraine, the State Service of Special Communication of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, the Ministry of Defense of Ukraine and other public authorities.

The basis for the development of this document was primarily the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine of September 14, 2020 № 392 (Decree of the President of Ukraine № 392/2020, 2020); experience of the best world practices (conceptual provisions of cybersecurity strategies of the EU countries, the EU itself, the USA, Japan, etc. were studied); a number of sociological surveys, empirical studies, etc.

The purpose of the Cyber Security Strategy of Ukraine is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. The document is based on the principles of deterrence, cyber resilience and interaction. The coordinator of the Strategy implementation is the National Cyber Security Coordination Center.

The said legal act states that cyberspace, along with other physical spaces, is recognized as one of the possible theaters of war. The trend of creating cyber troops is gaining momentum, which aims not only to protect critical information infrastructure from cyber attacks, but also to conduct preventive offensive operations in cyberspace, which includes the decommissioning of critical enemy infrastructure by destroying information systems that manage such objects. It was stated that the Russian

Federation remains one of the main sources of threats to national and international cybersecurity. This country is actively implementing the concept of information warfare, based on a combination of destructive actions in cyberspace and information and psychological operations, the mechanisms of which are actively used in the war against Ukraine. Such destructive activity poses a real threat of acts of cyberterrorism and cyber diversion against the national information infrastructure.

It is expected that in the first year of the Strategy indicators for assessing the state of cybersecurity and cybersecurity will be developed; a review of the state of cyber protection of critical information infrastructure, state information resources and information, the protection of which is established by law; mechanisms for reviewing the state of the national cybersecurity system have been developed and implemented. This will allow to optimally take into account changes in the security environment and adjust the overall plan and annual action plans for the implementation of the Strategy.

According to the approved Strategy, Ukraine will create the most open, free, stable and secure cyberspace in the interests of human rights and freedoms, social, political and economic development of the state.

To build the capacity of deterrence (C), the focus is on achieving the following strategic goals:

- goal C.1. Effective cyber defense;
- goal C.2. Effective countering of intelligence and subversive activities in cyberspace and cyberterrorism;
- goal C.3. Effective fight against cybercrime;
- goal C.4. Development of asymmetric containment tools.

To gain cyber resilience (K) it is necessary to achieve the following strategic goals:

- purpose K.1. National cyber readiness and reliable cyber defense;
- purpose K.2. Professional development, cyber-knowledge society and scientific and technical support of cybersecurity;
- goal K.3. Secure digital services.

To improve interaction (B) it is necessary to achieve the following strategic goals:

- goal B.1. Strengthening the coordination system;
- goal B.2. Formation of a new model of relations in the field of cybersecurity;
- goal B.3. Pragmatic international cooperation (Decree of the President of Ukraine).

However, in our opinion, the provisions of the new version of the Cyber Security Strategy of Ukraine should specify and detail the tasks set by Ukrainian law on:

- creation of a modern national cybersecurity system of the state;
- organization and ensuring the development of this system and functioning in the interests of national security of the state;
- preparation for repulse of military aggression in cyberspace (preparation and conduct of cyber defense).

In order to increase the efficiency of the information space protection system, it is considered appropriate:

- clarify existing approaches to creating a national cybersecurity system, taking into account trends in the security environment and best practices in cybersecurity of the world's leading countries;
- to focus the efforts of cybersecurity entities on acquiring the necessary capabilities for the quality of the tasks assigned to them, the creation and development of appropriate organizational structures (staffing, training and comprehensive support);
- master modern forms and methods of preparation and implementation of cybersecurity measures;
- intensify cyber defense and cyber defense in proportion to the growing level of threats, especially in the context of the preparation and implementation of enemy military aggression in cyberspace;
- respond in a timely and adequate manner to current cybersecurity threats by preventing, early detection, early response to them, elimination (minimization, elimination of consequences) of their impact;
- to improve the cybersecurity management system with its further integration into the public administration system;
- to establish cooperation (implementation of joint projects and activities, cooperation) within the framework of authority with the subjects of national security, as well as with NATO, the European Union, Partner countries in the joint implementation of cybersecurity tasks.

Given that Ukraine has committed itself to NATO and Partner countries in implementing modern approaches to cybersecurity, developing the necessary capabilities of the security and defense sector for action in cyberspace, and establishing interoperability in cybersecurity with the Alliance, In 2021, the President of Ukraine - V. Zelensky announced the creation and start of the Centers for Cyber Security and Countering Disinformation (ZCA, 2021).

It is planned that in order to fulfill the strategic objectives, these Centers will cooperate with the special services of foreign partner countries.

The main vector of such interaction should be aimed at eliminating the main threats to information security of states directly in cyberspace. These include:

- systemic and large-scale actions in cyberspace, which are resorted to by representatives of special services of foreign countries, officials of non-governmental organizations, including in the way of using special means of active influence in cyberspace (the use of cyberweapons);
- use of cyberspace capabilities for information and cyberspace;
- destructive impact on the objects of critical infrastructure of Ukraine in cyberspace during armed aggression, hostilities, terrorist attacks, sabotage, etc;
- awareness of the enemy about the vulnerability of information technology and information infrastructure for management in priority areas of life, ensuring proper defense of the state and its security;
- establishing cooperation and capacity building by states on cyber influence;
- development of organizational components of cyber structures of leading European states, purposeful involvement of non-state resources in participation in measures to ensure cybersecurity;
- development of cyber weapons and its application to perform tasks in cyberspace;
- stepping up efforts to focus on preventing covert illegal cyber attacks and cyber operations;
- enhanced influence on the national information spaces of other countries, network traffic by means of access to global information networks;
- development of information technologies on a global scale, including in the interests of cyber defense, cyber influence, cyber operations in general.

In organizing cooperation and establishing international cooperation in this area, it is necessary to take into account the provisions of the Convention on Cybercrime (adopted by the Council of Europe in 2001 and ratified by Ukraine in 2005, then the Budapest Convention), which is one of the first international regulations definition of «cybercrime» and forms an idea of crime in cyberspace (Law No 2824-IV, 2001). Today, the Budapest Convention is a fundamental document for the development of international and national legislation governing the fight against cybercrime.

The main EU acts in the field of information space protection are: EU Law «On ENISA (European Union Agency for Cyber Security) and on certification of cyber security of information and communication technologies and repeal of Regulation (EU) № 526/2013 (Law on Cyber Security)» of 17.04. 2019 (Law «On ENISA and certification»); Directive on measures for a high common level of security of network and information systems in the Union (Directive (EU) 2016/1148, 2016) of 06.07.2016; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General data protection provisions) Data Protection Regulation, GDPR) and others.

The EU has a key role to play in encouraging and supporting the development of cybersecurity capabilities in public and private bodies in the Member States, as well as in the European institutions themselves, building on European know-how. The EU can also provide support in the field of training and education, which creates synergies and prevents duplication of capacity.

Thus, cybersecurity encompasses all security measures that can be taken to protect against attacks in the digital space. The steady increase in the complexity and intensity of cyber attacks has led most developed countries to increase resilience and adopt national cybersecurity strategies in recent years. In particular, France has the National Cyber Strategy of 2011, the National Digital Security Strategy of 2015, and the International Digital Strategy of France of 2017. These documents are complemented by the White Paper, the Defense Review and the Cyber Defense Strategy Review. France's Internet environment is protected by public authorities such as ANSSI, CERT, COSSI, the Ministry of Defense, COMCYBER and the Ministry of the

Interior. Cybersecurity is considered by France to be a national priority for all its citizens today.

The German model of information security of the state operates on the basis of the Constitution of Germany, federal and state laws, decisions of constitutional courts, supranational legislation and relevant bylaws.

In particular, according to paragraph 1 of Article 5 of the Constitution of Germany, everyone has the right to freedom of expression and dissemination of opinion orally, in writing and through visual means, to freely receive information from all publicly available sources. Freedom of the press and freedom to transmit information through radio and cinema are guaranteed. Censorship is not carried out.

In 2009, the Constitution of Germany was supplemented by Article 91c, which laid the foundation for cooperation between the federal government and the state governments in the field of information technology. This provision is broad given the constant progress of information technology and its growing importance for public administration. It includes factual and legal aspects of such cooperation, establishes the possibility of harmonizing standards for their uniform application to ensure compatibility and security requirements in data exchange.

The basic law in the field of information security in Germany is the Law on Strengthening the Security of Information Technology Systems (Law on IT Security) of 25.07.2015. The law assigns the Federal Office for Information Technology Security (BSI) a central role in protecting critical infrastructures in Germany. Critical infrastructures are facilities, installations or parts of them that belong to the sectors of energy, information technology and telecommunications, transport and road transport, healthcare, water supply, food, finance and insurance. Such facilities are essential to the community because shutting them down or deteriorating them will lead to significant supply shortages or threats to public safety.

One of the fundamental legal documents in the field of information security in Spain is the National Cyber Security Strategy (Presidente del Gobierno, 2013). This act is the legal basis for the Spanish Government in the context of implementing the National Security Strategy (2013) to protect the cyberspace of the state, in particular, the implementation of concerted and coordinated action to prevent and combat identified cyber threats and eliminate their consequences (Ministerio de Defensa de Espana, 2017).

At the same time, in the EU, given the need for the most effective cooperation in the field of information space security, the emphasis is on cooperation between different agencies and countries.

The EU plans to set up a new cyber unit to respond to cyberattacks, which will include special teams that can immediately come to the aid of victims of hacker attacks. As a result of cooperation, EU countries affected by cyberattacks will be able to turn to other EU countries for help, including rapid response teams that will repel real-time hacker attacks.

It is also planned to create an interactive platform for cybercrime police, cyber agencies, diplomats, military services and cybersecurity firms to coordinate response and resource sharing.

Among other things, the unit will prepare regular reports on threats to the information space, prepare and test crisis response plans, and establish information-sharing agreements between governments and private cybersecurity firms. The unit will also coordinate existing work between cyber agencies and authorities within the bloc. The need for coordination is due to the fact that despite the existence of specialized bodies in this area, most EU countries face cyber attacks on their own, and their ability to counter such threats varies widely. It is planned that the unit will be fully operational by the end of 2022 (EU, 2021).

Conclusions

After analyzing the legal regulations and organizational aspects of information security in some European countries, we conclude that there is currently no unified model.

Given the dynamics of public relations in the information sphere, taking into account the need for effective measures to combat modern threats to information security, need to improve the form and methods of information protection, critical information infrastructure and information and psychological security of all European countries.

In our opinion, in order to organize effective international cooperation in the field of information space protection, efforts should be intensified in the following areas:

- improving coordination and cooperation within international organizations to strengthen cyber resilience - ensuring global, open, stable and secure cyberspace;
- strengthening the fight against cybercrime in Ukraine and the world;
- development of dialogue on cybersecurity and achievement of practical results of cooperation, etc.

Clearly, global capabilities to prevent, detect, mitigate, deter, respond to malicious cyber activity, and ensure the credible protection of states' information sovereignty need to be strengthened.

Thus the basic strategic purposes it is expedient to define:

- informing, advising, teaching and promoting in Ukrainian society the ideas and standards of information and cyberimmunity;
- cyber cooperation in providing modern services for cyber defense, especially areas vulnerable to conflicting states;
- application of modern approaches to the implementation of best practices at the state level (Ukraine needs to intensify cooperation with the European Union Network and Information Security Agency (ENISA), the European Center for Cybersecurity Research and Competences, and purposefully engage in EU joint coordination trainings the EU and Member States on large-scale cyber security incidents and crises;
- prevention of threats and challenges in the state with the use of cyberspace by the enemy;
- localization of challenges and threats to the state in cyberspace;
  deterring threats and challenges in cyberspace and through cyberspace;
  preparing the state to repel attacks in cyberspace in order to counter information aggression.

At the present stage, it is necessary to pay more attention to public-private partnerships as part of the institutional support of information and cybersecurity management.

Such a partnership should be implemented in the following areas:

- preparation of proposals for the development of strategic documents in the field of cybersecurity;
- participation in the development of national and international standards;
- ensuring the implementation of the advisory function;
- extensive consultations with stakeholders within advisory bodies;
- scientific and technical cooperation (state - scientific circles, scientific circles - business).

Bibliographic references

Chernysh, R., & Osichnyuk, L. (2021). National interests of the state and the possibility of restricting the right to freedom of speech: the question of correlation. Problems of Legality, (155), 166–181. https://doi.org/10.21564/2414-990X.155.243660. (In Ukranian)

Chernysh, R., Pogrebnaya, V.L., Montrin, I.I., Koval, T.V., & Paramonova, O.S. (2020) Development of Internet communication and social networking in modern conditions: institutional and legal aspects. Revista San Gregorio (special issues Nov). Url: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1572

Decree of the President of Ukraine № 392/2020. National Security Strategy of Ukraine, September 14, 2020. Retrieved from: https://www.president.gov.ua/documents/3922020-35037 (In Ukranian)

Decree of the President of Ukraine № 447/2021. On the Cyber-Security Strategy of Ukraine, August 6, 2021. Retrieved from: https://www.president.gov.ua/documents/4472021-40013 (In Ukranian)

Directive (EU) 2016/1148. Of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016. L. 194. P. 1–30. Retrieved from https://www.enisa.europa.eu/topics/nis-directive

EU (2021). EU to launch rapid response cybersecurity team. Retrieved from: https://www.politico.eu/article/eu-joint-cyber-unit-rapid-response-cyberattacks/

Law No 2824-IV. Convention on Cybercrime, September 7, 2005. Retrieved from http://zakon.rada.gov.ua/laws/show/994_575\ (In Ukranian)

Ministerio de Defensa de Espana (2017), «Estrategia de Seguridad Nacional», Retrieved from: https://www.dsn.gob.es/es/estrategias-

publicaciones/estrategias/estrategia-seguridad-nacional-2017

Ministry of Foreign Affairs of Ukraine (2021). Ukraine and the EU have launched a Cyber Dialogue. Retrieved from https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog (In Ukranian)

Pohoretskyi, M., Cherniak, A., Serhieieva, D., Chernysh, R., & Toporetska, Z. (2022). Detection and proof of cybercrime. Amazonia Investiga, 11(53), 259-269. https://doi.org/10.34069/AI/2022.53.05.26

Presidente del Gobierno (2013). «Estrategia de Ciberseguridad Nacional», Retrieved from: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Onyshchuk, S.V., Onyshchuk, I.I., Petroye, O., & Chernysh, R. (2020). Financial Stability and its Impact on National Security State: Organizational and Legal Aspects. International Journal of Economics and Business Administration, Volume VIII, Issue 1, pp. 353-365.

Tkachuk T. (2017). Ensuring information security in Central Europe. Legal Scientific Electronic Journal, № 5, S. 104–110. (In Ukranian)

Vlasenko, T.O., Chernysh, R.F., Dergach, A.V., Lobunets, T.V., & Kurylo, O.B. (2020). Investment Security Management in Transition Economies: Legal and Organizational Aspects. International Journal of Economics and Business Administration, Volume VIII, Issue 2, pp. 200-209.

ZCA (2021) Zelensky and the Cyber Army: How will Ukraine defend itself against Russia's digital attacks? Retrieved from: https://www.radiosvoboda.org/a/zelensky-viyna-kiberviysko-kiberbezpeka-hybrydna-viyna-rossiya--kytay/31592752.html (In Ukranian)