УДК 342.9

Leontii CHYSTOKLETOV
Lviv Polytechnic National University,
Professor of the Department
of administrative and informational law,
Educational and scientific institute of law,
psychology and innovative education,
Doctor of law, Professor,
e-mail: leontii.h.chystokletov@lpnu.ua,
ORCID: https://orcid.org/0000-0002-3306-1593

FEATURES OF ORGANIZATIONAL AND LEGAL PROVISION OF INFORMATION SECURITY IN THE CONDITIONS OF WAR WITH RUSSIA

http://doi.org/10.23939/law2024.41.365

The article, based on a theoretical and practical study of the essence and features of the regulation of information and legal relations in the conditions of russian aggression, focuses on the problematic issues of organizational and legal provision of information security as an activity aimed at the prevention, timely detection and termination of threats that destructively affect vital interests of the individual, society and the state in the information sphere.

It has been proved that the analysis of the results of the adoption of international legal acts by the UN General Assembly in recent years, with their short-sighted and futile vision, confidently prove that the entire burden of the organizational and legal provision of information security in the formation of principled positions on the regulation of norms aimed at the development of a single mechanism in counteracting threats to geopolitical information security still rests with states within their territorial jurisdiction.

It has been determined that the informational pressure, which russia has continuously been using against Ukraine over the past decade, is being accompanied by frantic information propaganda aimed at discrediting public authorities, baseless accusations of the Armed Forces of Ukraine for the deaths of people in the temporarily occupied territory, and the imposition of the chauvinistic idea of defending "russian" peace", the return of the post-Soviet republics to the "renewed Union" with its imperial goals of aggression.

Taking into account the problems of organizational and legal provision of information security, an analysis of the implementation of legal acts regulating informational and legal relations in the conditions of the russian-Ukrainian war has been carried out. Attention has been drawn to the order of creation and running of the system of operational and technical management of electronic communication networks of public use and the national centre of management of electronic communication networks for the purposes of defence and security of the state in conditions of martial law.

The issues of combating phishing as a form of information attack, which, having been presented as a simple electronic message, is carried out by criminal groups in a deceptive way

on the user in order to obtain any type of data, have been studied out. The problems associated with the implementation of the filtering system for phishing domains, which may create additional significant risks and pose threats to the information security of Ukraine, have been outlined. The mechanisms of organizational and legal protection against disinformation and the means of countering it have been defined.

Taking into account the recommendations of the numerous scientists and practitioners, proposals have been made to optimize the organizational and legal provision of information security in the conditions of russian aggression.

Key words: russian aggression; organizational and legal support; information security; threat; information propaganda; phishing; disinformation.

Problem formulation. The growth course of the full-scale russian invasion in Ukraine indicates the enemy's unceasing use of the latest information technology to exert anti-Ukrainian informational influence, which has a destructive effect on the mechanism for regulating informational and legal relations in wartime conditions. In the context of the implementation of these events, a special role is played by information law, which, like other areas of law, is going through difficult times of development, testing, search and improvement, aimed at optimizing the model of legal provision of information security in relation to the protection of the rights, interests of citizens, society and the state.

Research of the paradigm of legal provision of information security in the modern development of our society allows us to fully define the concepts and the main vector of transformations, in the centre of which there are notions of "information", "organizational and legal provision", "security", "cyber security", "cyber protection", "struggle with disinformation" which include a system of counteracting external and internal threats that encroach on the democratic development of Ukraine.

Analysis of the study problem. Definition of the mechanism of administrative and legal provision of information security, its essence and individual aspects were covered by K. Belyakov, O. Dovgan, O. Zolotar, A. Marushchak, V. Pylypchuk, T. Tkachuk and others. However, scientific studies of the problems of organizational and legal provision of information security in the conditions of the war with russia have been ignored greatly. Therefore, improving the information potential of our country requires careful research and study, which actualizes the topic of this work.

The purpose of the article. The purpose of the article is to study the problems of organizational and legal provision of information security in Ukraine, to determine the ways of its optimization in the conditions of the russian-Ukrainian war as one of the fundamental areas of activity of public authorities in the field of protection of the domestic information space.

Presentation of the main material. The semantics of the concept of war and peace, which is chronicled throughout the historical development of Ukraine in the neighbourhood with the russian enemy, has always been characterized by the boundless courage and heroism of the Ukrainian people in the struggle for their independence. And in the present time, commemorating the memorable 242-day immortal resistance of Ukrainian cyborgs, who courageously defended the Donetsk airport from russian aggressors, despite the insane informational pressure to surrender, once again demonstrated the remarkable heroism of the Armed Forces of Ukraine – the descendants of the Zaporizhsky Cossacks. As history shows, throughout its existence, Ukraine has always been proud of the courage and fortitude of its heroes. In confirmation of this, in the 17th century, in the russian-Turkish war of 1768–1774, during the fighting on the Danube, the Zaporizhska flotilla captured dozens of Turkish ships of various types, numerous guns, weapon, ammunition, destroyed and captured thousands of Turkish soldiers. And on January 5, 1771, not russian officers, but only representatives of the Ukrainian Cossacks led by Peter Kalnyshevskyi and 16 senior officers of Zaporizhska Sich were awarded a gold medal with diamonds for their military merits. [1].

Features of organizational and legal provision of information security in the conditions of war with Russia

Today, information security issues are of great interest not only to individual countries, but also to the entire world. One of the first international legal acts, in which the problems of information security were outlined, are Resolutions of the UN General Assembly A/RES/53/70 of December 4, 1998 "Achievements in the field of informatisation and telecommunications in the context of international security" [2] and 54 / 49 of December 1, 1999 "Achievements in the field of informatisation and telecommunications in the context of international security" [3], which indicated the negative impact of information and communication technologies (hereinafter – ICT), which can harm the international stability and security of states and, first of all, the civil and military spheres. We find a more updated conceptual approach to the issues of ensuring international information security in the Report of the Group of Governmental Experts on Achievements in the Field of Informatisation and Telecommunications in the Context of International Security Resolution GA/70/174 dated June 22, 2015 [4], the content of which is aimed at countermeasures to the existing threats associated with the buildup of military potential in the field of ICT, which makes its use in future conflicts between states more likely, in particular, by attacking important infrastructure facilities.

Continuing the development of the specified issues, the international community at the UN General Assembly A/RES/76/19 of December 6, 2021 "Achievements in the field of informatisation and telecommunications in the context of international security and encouraging the appropriate behaviour of states in the use of information and communication technologies" [5] it was recommended for independent states to adhere to proposals on security issues in the field of ICT use for the years 2021–2025.

However, the analysis of the results of the adoption of international legal acts by the UN General Assembly in recent years, with their short-sighted and futile vision, confidently prove that the entire burden of the organizational and legal provision of information security in the formation of principled positions regarding the regulation of norms aimed at the development of a single mechanism in countermeasures threats to geopolitical information security still rests with states within their territorial jurisdiction.

Modern military and political realities with the endless commission of military terrorist crimes by russia against the civilian population, with the destruction of civil infrastructure, using psychological methods and means of influencing the consciousness of citizens, are accompanied by frantic information propaganda aimed at discrediting public authorities, imposing a chauvinistic idea of the defence of "russian peace", the return of the post-Soviet republics to the "renewed Union" with its imperial invasive purposes.

Returning to our realities, in the conditions of today's russian aggression, our country faces a difficult task in the information confrontation with russia, which is becoming a fundamentally new sphere of rivalry not only with Ukraine, but also between all the countries of the world. At the same time, it is no secret that the state of organizational and legal provision of information security before the large-scale russian aggression against Ukraine was not satisfactory. As stated in the decree of the President of Ukraine On the decision of the National Security and Defence Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine" <...> "The absence of a comprehensive information policy of the state, the weakness of the strategic communications system make it difficult to neutralize this threat" [6].

Under today's conditions of russian occupation, public authorities, through information and communication support, with the financial support of the international community, direct measures for the survival of the state, society and citizens, strengthening the lost military potential of the Armed Forces of Ukraine, further overcoming the enemy and rebuilding the country. However, before the full-scale military aggression of russia against Ukraine in the period 2014–2022, the main task in the information protection of the state was the formation of an effective mechanism for the legal provision of information security in peacetime – and few of the state authorities assumed the idea of the possibility of a terrible military invasion from the side our eastern neighbour.

In general, despite a certain imbalance, declarative nature and short-sightedness of the regulatory system of domestic information legislation, the organizational and legal provision of information security has been reformatted in recent years in accordance with modern challenges and threats in the conditions of the russian-Ukrainian war.

During this period, after the adoption of practical steps regarding the organizational and legal provision of information security, the first normative legal acts in this area were aimed at regulating the essence and improving the means of implementing information protection. These include the Law of Ukraine "On the National Security of Ukraine" dated June 21, 2018, in which, among the main tasks of the national security of Ukraine, existing and potentially possible cyber threats to the vital interests of people and citizens, society and the state in cyberspace are identified, priority directions, conceptual approaches to the formation and the implementation of state policy regarding the safe functioning of cyberspace, its use in the interests of the individual, society and the state, increasing the effectiveness of the main subjects of cyber security, primarily subjects of the security and defence sector... [7].

The National Security Strategy of Ukraine, put into effect by the decree of the President of Ukraine On the decision of the National Security and Defence Council of Ukraine dated September 14, 2020, outlines the priority tasks of law enforcement, special, intelligence and other state bodies in accordance with their competence, which are aimed at active and effective countermeasures intelligence and subversive activities, special information operations and cyber attacks, russian and other subversive propaganda [8].

The legal provisions of the Law of Ukraine "On Electronic Communications" reveal the essence of creating the basis for effective and harmonised use of the radio frequency spectrum, ensuring economic, social, information and cultural development, state security, defence capability, fulfilment of international obligations, as well as ensuring and protecting the interests of the state and users of the radio frequency spectrum. No. less remarkable powers in this area are vested in the CM of Ukraine, which is responsible for approving the procedure for the establishment and operation of the system of operational and technical management of public electronic communication networks and the national centre for the management of electronic communication networks for the purposes of defence and security of the state in an emergency, state of emergency or martial law [9].

Subsequently, on 15 October 2021, the National Security and Defence Council of Ukraine approved the Information Security Strategy, enacted by the Decree of the President of Ukraine of 28 December 2021 No. 685/2021, which aimed to strengthen the capacity to ensure the information security of the state, its information space, support by information means and measures of social and political stability, state defence, protection of state sovereignty, territorial integrity of Ukraine, democratic constitutional order, ensuring the rights and freedoms of every citizen. The main provisions of the Law of Ukraine "On the National Informatisation Programme" of 1 December 2022 No. 2807-IX reveal a set of tasks, programmes, projects, and works on informatisation aimed at developing the information society through the concentration and rational use of financial, material, technical and other resources, the production and scientific and technical potential of the state, coordination of activities of state bodies, local governments, as well as enterprises, institutions, and organisations regardless of the form of property [11].

In order to reduce the flow of false information within our country and increase the level of information security, on March 22, 2022, the President of Ukraine signed Decree No. 152/2022 to implement the decision of the National Security and Defence Council of Ukraine "On the Implementation of the Unified Information Policy under Martial Law". The main purpose of the decree is to unite on a single information platform all national TV channels, the program content of which mainly consists of strategic communication of information or information and analytical programs [12].

Also of great interest we consider the Order of the Cabinet of Ministers of Ukraine of 30 March 2023 No. 272-p. "On Approval of the Action Plan for the Implementation of the Information Security Strategy for the Period up to 2025", which was adopted pursuant to the decision of the National Security and Defence Council of Ukraine of 15 October 2021 "On the Information Security Strategy", enacted by the Decree of the President of Ukraine of 28 December 2021 No. 685/2021 (hereinafter – the Order). The purpose of the Order is to create conditions for ensuring the information security of Ukraine, aimed at protecting the vital interests of the citizen, society and the state in countering internal and external threats,

ensuring the protection of state sovereignty and territorial integrity of Ukraine, maintaining social and political stability, state defence, ensuring the rights and freedoms of every citizen [13].

At the same time, despite the whole range of activities of public authorities aimed at bringing the mechanism of organisational and legal support of information security to a reasonable model of its regulation, the information space in the context of russian aggression keeps "presenting" us with new challenges and threats. Phishing, which we believe is a form of information attack using social engineering disguised as electronic messages, is no exception in this regard, and is used by criminal groups to deceive users into obtaining any type of data. At first glance, the files requested by phishing sites appear to be safe, as their content is limited to obtaining scant information about the user's birthday, name, mother's maiden name, credit card or bank account number, etc. However, once such requests are opened, a malicious program is launched, which gives attackers access to the information they need or can even paralyse a wide range of IT system operations. An analysis of information on the number of phishing attacks shows that since the beginning of russia's large-scale invasion, the number of phishing attacks in Ukraine has increased by one and a half times. Thus, according to the State Service of Special Communications, the number of phishing attacks on the public sector in 2019 was 1,276,283, in 2020 – 4,641,791, in 2021 – 678,814, in 2022 – 9,549,384, and in 2023 – 433,160. The number of phishing attacks detected in publicly available sources: in 2019 – 8, in 2020 – 7, in 2021 – 10, in 2022 – 15, in 2023 – 17 [14].

The authority for the organisational and legal provision of countering phishing attacks on the public sector is entrusted to the State Special Intelligence Service, and the investigation of such crimes is carried out by the Cyber Police Department of the National Police. Only in the period from January to May 2023, the Cyber Police Department of the National Police received more than 15,000 complaints from citizens who were affected by phishing attacks [15].

Despite the assertion of some lawyers that phishing does not belong to a crime, nor to an administrative, nor to a disciplinary offence [16], the Criminal Code of Ukraine (hereinafter – the Criminal Code) provides for three criminal law norms, according to which objective and subjective signs of the crime may be brought to criminal responsibility, which are defined in the next Articles [17]:

– Article 361 of the Criminal Code – unauthorized interference in the work of informational (automated), electronic communication, informational and communication systems, electronic communication networks;

– Article 361-1 of the Criminal Code – creation for the purpose of illegal use, distribution or sale of malicious software or technical means, as well as their distribution or sale;

– Article 363-1 of the Criminal Code – interfering with the operation of electronic computing machines (computers), automated systems, computer networks or telecommunications networks by mass distribution of telecommunications messages.

But as the practice shows when investigating crimes for phishing attacks, law enforcement officers have to face a number of factors related to the impossibility of establishing the fact of information blocking, distortion of the information processing process or violation of the established order of its routing, its leakage, loss, forgery, etc.

According to Article 32 of the Law of Ukraine "On Electronic Communications", the Decree of the President of Ukraine dated 24.02.2022 No. 64/2022 "On the introduction of martial law in Ukraine", approved by the Law of Ukraine dated 24.02.2022 No. 2102-IX "On the Approval of the Decree of the President of Ukraine "On the introduction of martial law in Ukraine" (with amendments), in response to the request of the National Security and Defence Council of Ukraine regarding the implementation of a phishing domain filtering system as a component of the National Domain Name Service (DNS) by the National Centre for Operational-Technical Management of Telecommunications Networks of the State Special Communications Service of January 30 In 2023, the dubious order No. 67/850 "On the Implementation of the Phishing Domain Filtering System" was issued. In order to combat fraud in the banking and financial spheres related to the use of phishing Internet resources, the Regulation defines the principles and procedures for interaction with the filtering system of phishing domains [18].

However, in April 2023, the Internet Association of Ukraine (hereinafter referred to as the Internet Association of Ukraine) conducted a survey on the risks of the Phishing Site Filtering System, which was implemented by the Decree of the Ukrainian National Security Agency. 78 heads of enterprises, representing the majority of electronic communications operators, took part in the survey, among whom 62 % of the surveyed operators believe that the domain blocking system introduced by the order poses threats to the information security of Ukraine, and 72 % of the respondents believe that the use of the "transit" server of the National Coordination of the Cyber Security Centre at the National Security and Defence Council of Ukraine to transfer to providers the list of phishing sites formed by the CSIRT team of the NBU, creates additional significant risks [14].

Thus, in the opinion of INSAU specialists, instead of an automatic system, an alternative system for blocking phishing sites should be created with the possibility for each provider to review the list of sites to be blocked in case of an error. Relevant proposals and comments of the INSAU were submitted for consideration by the NSDC and relevant state bodies. Currently, the NSDC is considering the proposals of the INSAU regarding changes to the Regulations for the operation of the phishing domain filtering system, which are necessary to exclude damage to the information security of Ukraine by the phishing domain filtering system, to prevent the illegal collection and use of users' personal data, and to reduce the risks of extrajudicial blocking of sites that are not phishing [19].

It is worth mentioning that in March 2023, during the monitoring of judicial practice, experts found 86 verdicts in criminal cases directly related to issues of freedom of expression, and in 34 of them there are facts of possible violations of digital rights [16].

Now regarding the study of the issue of disinformation as one of the main directions of russian propaganda, the strengthening of which in Ukraine negatively affects the state of information security. According to the monitoring data of the Human Rights Platform, in March 2023, the russians were actively spreading disinformation: in total, Ukrainian experts discovered 157 disinformation messages on 19 topics, including five new ones for russian propaganda [20]. According to statistics, [14] the number of disinformation messages detected in the media between January 2023 and August 2023 (1,454 messages) doubled, compared to 742 between February 2022 and December 2022. At the same time, in the period from 2019 to 2021, a total of 71 disinformation messages were found in publicly available sources, which illustrates both the growth of the wave of disinformation after a full-scale invasion, and the number of projects in Ukraine aimed at detecting and countering it.

It is also not a secret concerning which spheres of life the attacks of russian disinformation are aimed at. As evidenced by russia's practice of disseminating false information, it is associated with disinformation about:

– Ukraine, its name and origin, and that it "does not have its statehood and sovereignty";

– critical state of health of the President of Ukraine, discrediting the activities of his office and public authorities;

– supply of prohibited weapons to Ukraine by the West;

– inciting religious enmity between the Ukrainian Church and the Church of the Moscow Patriarchate;

– the existence of biological laboratories on the territory of Ukraine aimed, with the help of pigeons and some other poultry, at causing a biological attack on russia;

– the existence of Nazism in Ukraine;

– the threat of russia using nuclear weapons;

– accusation of the activities of the Armed Forces of Ukraine. An example of this is the accusation of the Armed Forces of Ukraine that on January 21, 2024, a missile attack was carried out on the trading market of the Donetsk region, as a result of which 25 citizens were allegedly killed and 27 injured. This thesis was quickly picked up by Reuters journalists and immediately the "talking head of russia" – Serhiy Lavrov flew to the UN, regarding the convening of a meeting from this fabricated "russian theatrical performance". However, as it turns out from the information of the Armed Forces of Ukraine and the

residents of this neighbourhood themselves, the rockets were fired from the territory previously captured by the russian troops – the Chervonogvardiyska Mines, in order to once again blame the Armed Forces of Ukraine and its command for the deaths of the civilians. It's a matter of fact that the same situation is with the representing of the events of the russian-Ukrainian war in foreign media (especially in the US press) with reference to the russian media regarding the accusation of the Armed Forces of Ukraine for the deaths of residents of the occupied territory.

By the way, the absurd idea of the "russian world" was spread through information propaganda. The continuation of this informational lie was reflected in the events surrounding russia's violent annexation of Crimea in 2014, when it took advantage of the moment of change of power in Ukraine, as a result of Euromaidan, to occupy the Crimean peninsula – and these criminal actions are now being interpreted by the Russian authorities as "the return of Crimea to russia"!

According to historical chronicles, Crimea was first seized by russia in 1774 during the russian-Turkish War. However, the obligations resulting from the peace agreement signed between russia and the Ottoman Empire regarding the withdrawal of russian troops from Crimea were never fulfilled. The russian Empire, by inciting enmity between the ruling elite of Crimea, constantly interfering in its internal affairs, adopted a dubious manifesto, which subsequently led to the annexation of the Crimean Khanate, turning it into part of its territory. By analogy, the text of the 1783 manifesto "On the Acceptance of the Crimean Peninsula, Taman Island and the Entire Kuban Side, under the russian State" is no different from the brazen law on the Second Annexation of Crimea signed by Putin "On the Acceptance of the Republic of Crimea into the russian Federation and the Formation of New Subjects within the russian Federation – the Republic of Crimea and the City of Federal Significance Sevastopol". As you can see, the two historical chronologies of the annexation of Crimea in 1783 and in 2014 once again point to the imperial aggressive nature of russia, whose military and political strategy has not changed over the history of its existence, but has become more hostile and criminal.

The provisions of the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392, are an important lever in the mechanism of organizational and legal provision of information security. In addition, with the aim of countering current and projected threats to national security and national interests of Ukraine in the information sphere, effective countering of propaganda, destructive disinformation influences and campaigns, prevention of manipulation of public opinion By Decree of the President of Ukraine of March 19, 2021 No. 106/2021, in accordance with the decisions of the National Security and Defence Council, the Centre for Combating Disinformation was established [21]. The main tasks of the Centre are:

– analysis and monitoring of events and phenomena in the information space of Ukraine, the state of information security and the presence of Ukraine in the world information space;

– identification and study of current and projected threats to Ukraine's information security, factors affecting their formation, forecasting and assessment of consequences for the security of Ukraine's national interests;

– providing the National Security and Defence Council of Ukraine, the Chairman of the National Security and Defence Council of Ukraine with informational and analytical materials on the issues of ensuring the information security of Ukraine, identifying and countering disinformation, effectively countering propaganda, destructive informational influences and campaigns, preventing attempts to manipulate public opinion;

– preparation and submission of proposals to the National Security and Defence Council of Ukraine, the Chairman of the National Security and Defence Council of Ukraine [22].

Regarding the qualification of responsibility for disinformation, domestic legislation does not use the term "disinformation" itself, with the exception of Part 5 of Article 89 of the Law of Ukraine "On Media" where it is indicated "...countering the spread of disinformation during the preparation and holding of the referendum, ensuring the transparency of campaigning on platforms, in particular by introducing campaign labelling and introducing special notifications..." [23]. However, the Constitution and the Law of

Ukraine "On Media", Law of Ukraine "On Information", Code of Ukraine on Administrative Offences (hereinafter – CPA), CCU prescribe procedures for responding to the spread of false and unreliable information. We have to admit that Part 4 of Article 32 of the Constitution of Ukraine guarantees everyone judicial protection of the right to refute inaccurate information about himself and his family members and the right to demand the removal of any information, as well as the right to compensation for material and moral damage caused by the collection, storage, use and distribution of such inaccurate information [24]. In accordance with criminal legislation, the Criminal Code prohibits the dissemination of false or unreliable information in 15 articles (Articles 109–111, Part 1 of Article 111-1, 114-1, Part 1 of Article 114-2, Part 2 of Article 114-2, 161, 235-1, 236-2, 258-2, 295, 436, 436-1, 442 of the Criminal Code), in which criminal acts are connected with the phrases such as: "public appeals to...", "damage to sovereignty...", "obstructing legal activity...", "the dissemination of which is aimed at..." etc. [25]. As for administrative responsibility, in Article 173-1 of the Civil Code, it has been established for the dissemination of false rumours that may cause panic among the population or violation of public order, regardless of the method of such dissemination (orally, through social networks on the Internet, by posting information in public places, etc.) [26].

In addition to the specified legislation, the mechanism of organizational and legal support can be strengthened with the adoption of the draft law "On countering disinformation" [27], providing the introduction of the position of the Information Commissioner, who, in particular:

– will monitor the information space;

– will respond to claims of misinformation;

– will contact the disseminators of information for the reply or refutation of misinformation;

– will apply to the court with applications to limit access to information in the absence of original data of the distributor or lack of response to his applications, and with claims for refutation and granting the right to answer regarding misinformation;

– will contact law enforcement agencies in case of signs of a criminal offence.

The draft law also defines the term "disinformation", and also proposes to establish administrative liability for the dissemination of disinformation, violation of the rules of refutation, providing an answer and transparency requirements, and criminal liability for the systematic and intentional mass dissemination of disinformation.

It is worth mentioning that in our time, when the geopolitical forces in the world are divided into two opposing camps due to the outbreak of wars in Ukraine and Israel, in Malta on October 28–29, 2023, with the participation of political advisers on national security issues from 66 countries – as a logical continuation of consultations in the appropriate format in Copenhagen (Denmark) in June and in Jeddah (Saudi Arabia) in August of this year, the third meeting on the Ukrainian peace formula of the President of Ukraine V. Zelensky was successfully held. And despite the fact that russian propaganda launched a real information attack to discredit the results of the summit, claiming that the mission of the Ukrainian peace forum was a failure, the meeting in Malta showed the broad support of Ukraine by the countries of the world and destroyed the russian myth about Ukraine's loss of support from the so-called Global South [28].

The study of the problems of organizational and legal provision of information security during the period of russian aggression revealed important challenges and opportunities for the protection of individuals, society and the state in the conditions of modern information and communication technologies. The given proposals and recommendations can serve as a basis for the development of new scientific developments in countering informational threats in the context of the russian-Ukrainian war.

Conclusions. Taking into account the proposals and recommendations of the numerous scientists and practitioners, the key measures of organizational and legal provision of information security in the conditions of russian aggression are:

– development and improvement of the modern system of regulatory and legal acts aimed at rapid and appropriate regulation of informational and legal relations;

– conducting fundamental, applied scientific research and scientific and technical (experimental) developments in the field of organizational and legal provision of information security;

– formation of international research institutions and institutions of the military-industrial complex, the activities of which should be aimed at the powerful production of modern radio-electronic means of anti-aircraft, ground defence and anti-aircraft missile systems;

– development of indicators for evaluating the effectiveness of information security threat notification and its protection systems;

– increasing, with the aim of countering russian propaganda, the potential of information and technical resistance to fakes and distortions of enemy information, capable of positively influencing the protection of Ukrainian statehood and independence;

– accumulation, redistribution and stable use of financial resources as fundamental means of material and technical support of the defence capability of the state and the Armed Forces.

The study of the problems of organizational and legal provision of information security during the period of russian aggression revealed important challenges and opportunities for the protection of individuals, society and the state in the conditions of modern information and communication technologies. The given proposals and recommendations can serve as a basis for the development of new scientific developments in countering informational threats in the context of the russian-Ukrainian war.

REFERENCES

1. Chuhlib T. V. Russian-Turkish War 1768–1774. URL: http://www.history.org. ua/ ?termin=Rosijsko _turetska_1768.

2. Achievements in the field of informatisation and telecommunications in the context of international security: Resolution A/RES/53/70 of the UN General Assembly of December 4, 1998. URL: https://documents-dds-ny.un.org/ doc/ UNDOC/ GEN/N99/760/05/PDF/N9976005.pdf?OpenElement.

3. Achievements in the field of informatisation and telecommunications in the context of international security: Resolution A/RES/54/49 of the UN General Assembly of December 1, 1999. URL: https://documents-dds-ny.un.org/doc/ UNDOC/ GEN/N99/777/15/PDF/ N9977715. pdf?OpenElement.

4. Report of the Group of Governmental Experts on Achievements in the Field of Informatisation and Telecommunications in the Context of International Security: Resolution of the UN General Assembly A/70/174 of June 22, 2015. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/ 37/PDF/N 1522837.pdf?OpenElement.

5. Achievements in the field of informatisation and telecommunications in the context of international security and encouraging appropriate behaviour of states in the field of information and communication technologies: UN General Assembly Resolution A/RES/76/19 of December 6, 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/ 51/PDF/N2137751. pdf?OpenElement.

6. On the National Security Strategy of Ukraine: decree of the President of Ukraine On the decision of the National Security and Defence Council of Ukraine dated September 14, 2020. URL: https://zakon.rada. gov.ua/laws /show/392/2020#Text.

7. On the National Security of Ukraine: Law of Ukraine dated June 21, 2018 No. 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

8. On the National Security Strategy of Ukraine: Decree of the President of Ukraine On the decision of the National Security and Defence Council of Ukraine dated September 14, 2020. URL: https://zakon.rada. gov.ua/laws/show/392/2020#Text.

9. On Electronic Communications: Law of Ukraine dated December 16, 2020 No. 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

10. On Information Security Strategy: Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. URL: https://www.president. gov.ua/ documents/ 6852021-41069.

11. On the National Informatisation Program: Law of Ukraine dated December 1, 2022 No. 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text.

12. Regarding the implementation of a unified information policy under martial law: Decree of the President of Ukraine dated March 19, 2022 No. 152/2022. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text.

13. On the approval of the plan of measures for the implementation of the Information Security Strategy for the period until 2025: Order of the Cabinet of Ministers of Ukraine dated March 30, 2023. No. 272-p. URL: https://ips.ligazakon.net/document/ KR230272?an=1.

14. War in the digital dimension and human rights: final report from February 24, 2022 to August 31, 2023 / O. Vdovenko. Kyiv: Human Rights Platform NGO, 2023. 84 p. URL. https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf.

15. Since the beginning of the year, the cyber police has received more than 15,000 complaints about phishing attacks. URL: https://zmina.info/news/vid-pochatku-roku-kiberpolicziya-otrymala-bilsh-yak-15-tysyach-zvernen-shhodo fishyngovyh-atak/.

16. Ukraine operates a filtering system for phishing domains: human rights defenders say that it is illegal and collects citizens' data. URL: https://zmina.info/news/v-ukrayini-praczyuye-systema-filtracziyi-fishyngovyh-domeniv-pravozahysnyky-kazhut-shho-vona-poza-zakonom-ta-zbyraye-dani-gromadyan/ю.

17. Criminal Code of Ukraine. URL: https:/ /zakon. rada. gov. ua/ laws/ show/ 2341-14#Text.

18. On the implementation of the phishing domain filtering system: Order of the National Centre for Operational and Technical Management of Telecommunications Networks of the State Special Communications Service of January 30, 2023 No. 67/850. URL: https://nkrzi. gov.ua/ images/news/ 11/2580/67_30012023.pdf.

19. The automatic filtering system, which is dangerous for national security, will be challenged in the courts. URL:https://inau.ua/news/novyny-inau/nebezpechnu-dlya-natsionalnoyi-bezpeky-systemu-avtomatychnoyi-filtra tsiyi.

20. Almost a third of verdicts in freedom of expression cases contain signs of digital rights violations – Human Rights Platform. URL: https://zmina.info/news/vyroky-u-spravah-shhodo-svobody-vyrazhennya-poglyadiv-platforma-prav-lyudyny/.

21. On the creation of the Centre for countering disinformation: decree of the President of Ukraine dated March 19, 2021 No. 106/2021. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21/print.

22. Regulations on the Centre for Combating Disinformation: Decree of the President of Ukraine dated May 7, 2021 No. 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text.

23. About media: Law of Ukraine of December 13, 2022 No. 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20?find =1&text=%D0%B4%D0%B5% D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96#w1_1.

24. Constitution of Ukraine. URL: https://zakon.rada.gov.ua/laws/ show/254%D0%BA/96-%D0%B2%D1%80#Text.

25. Criminal Code of Ukraine. URL: https://zakon. rada.gov.ua/laws/show/2341-14#Text.

26. Code of Ukraine on administrative offences. URL: https://zakon.rada.gov.ua /laws/show/80731-10#Text.

27. Criminal liability for the mass dissemination of disinformation. URL: https://lexinform.com.ua/zakonodavstvo/za-masove-poshyrennya-dezinformatsiyi-kryminalna-vidpovidalnist/.

28. How the meeting on Malta destroyed the myth about the loss of attention to Ukraine.URL: https://cpd.gov.ua/main/yak-zustrich-na-malti-zrujnuvala-mif-pro-vtratu-uvagy-do-ukrayiny/.

Дата надходження: 08.02.2024 р.

Леонтій ЧИСТОКЛЕТОВ
Національний університет "Львівська політехніка",
професор кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти,
доктор юридичних наук, професор,
e-mail: leontii.h.chystokletov@lpnu.ua,
ORCID: https://orcid.org/0000-0002-3306-1593

ОСОБЛИВОСТІ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ З РОСІЄЮ

У статті на підставі теоретичного та практичного вивчення сутності та особливостей регулювання інформаційно-правових відносин в умовах російської агресії акцентовано на проблемних питаннях організаційно-правового забезпечення інформаційної безпеки як діяльності,

спрямованої на запобігання, своєчасне виявлення та припинення загроз, які деструктивно впливають на життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.

Аналіз міжнародно-правових актів, прийнятих Генеральною Асамблеєю ООН за останні роки, з їх недалекоглядним та безперспективним баченням, впевнено доводить, що весь тягар організаційно-правового забезпечення інформаційної безпеки у формуванні принципових позицій щодо врегулювання норм, спрямованих на вироблення єдиного механізму протидії загрозам геополітичній інформаційній безпеці, як і раніше, покладається на держави в межах їхньої територіальної юрисдикції.

Визначено, що інформаційний тиск, який безперервно здійснює росія проти України упродовж останнього десятиріччя, супроводжується шаленою інформаційною пропагандою, спрямованою на дискредитацію органів публічної влади, безпідставне звинувачення ЗСУ у загибелі людей на тимчасово окупованій території, нав'язування шовіністичної ідеї відстоювання "руського миру", повернення пострадянських республік до "оновленого Союзу" з його імперськими загарбницькими цілями.

Враховуючи проблеми організаційно-правового забезпечення інформаційної безпеки, проаналізовано реалізацію нормативно-правових актів, які регулюють інформаційно-правові відносини в умовах російсько-української війни. Звернено увагу на порядок створення та діяльність системи оперативно-технічного управління електронними комунікаційними мережами загального користування та національного центру управління електронними комунікаційними мережами для цілей оборони та безпеки держави в умовах воєнного стану.

Досліджено питання протидії фішингу як форми інформаційної атаки, яку, маскуючись під електронні повідомлення, здійснюють злочинні групи, вводячи в оману користувача з метою отримання будь-якого типу даних. Окреслено проблеми, пов'язані із упровадженням системи фільтрації фішингових доменів, які можуть створювати додаткові істотні ризики та створювати загрози для інформаційної безпеки України. Визначено механізм організаційно-правового забезпечення протидії дезінформації та засоби її протистотяння.

З урахуванням рекомендацій більшості науковців та практиків надано пропозиції щодо оптимізації організаційно-правового забезпечення інформаційної безпеки в умовах російської агресії.

Ключові слова: російська агресія; організаційно-правове забезпечення; інформаційна безпека; загроза; інформаційна пропаганда; фішинг; дезінформація.