DOI: https://doi.org/10.34069/AI/2022.58.10.7

How to Cite:
Naidon, Y., Naumiuk, S., Rybynskyi, Y., Kravchenko, O., & Buriak, N. (2022). Destructive information influence and its implementation. *Amazonia Investiga*, *11*(58), 65-73. https://doi.org/10.34069/AI/2022.58.10.7

Destructive information influence and its implementation

Деструктивний інформаційний вплив та його реалізація

Received: October 3, 2022 Accepted: November 10, 2022

Written by:
Yuliana Naidon[27]
https://orcid.org/0000-0002-1076-0471
Serhii Naumiuk[28]
https://orcid.org/0000-0001-7039-0946
Yevhenii Rybynskyi[29]
https://orcid.org/0000-0001-6014-0142
Olena Kravchenko[30]
https://orcid.org/0000-0003-0246-1022
Nataliia Buriak[31]
https://orcid.org/0000-0001-5428-8087

Abstract

With the dynamic development of political, economic and military processes, the guarantee of the national security in the information space is an essential element that significantly changes the appropriate functioning of any country. The current state of affairs in the context of the mainstreaming of the Ukrainian factor in the information warfare requires improvements of state institutions to counter Russian Federation destructive informational influence and its special information operations. Taking into account theoretical and applied research on the issue, it is worth mentioning that destructive information impact requires a systematic and integrated approach to problem solving. In the research authors investigate theoretical aspects of destructive informational influence and determine prior directions of the use in information warfare against Ukraine by Russian Federation. Scientific methods of modern epistemology are applied in accordance with the aim of the research. On the methodological basis of the study, the cognitive theory as a fundamental principle is used by experts in the field of information security. The results of analysis of theoretical research aspects of Ukrainian and foreign scholars determine priorities for the enemy to use destructive

Анотація

В умовах динамічного розвитку політичних, економічних і військових процесів важливим компонентом, що суттєво впливає на забезпечення нормального функціонування будь-якої країни, є забезпечення її національної безпеки в інформаційній сфері. Реалії сьогодення у контексті актуалізації українського фактору в інформаційній війні вимагають удосконалення функціонування державних інституцій для протидії деструктивним інформаційним впливам з боку російської федерації та її спеціальним інформаційним операціям. Забезпечення ефективної протидії деструктивному інформаційному впливу вимагає системного і комплексного підходу для вирішення цієї проблеми, у тому числі з урахуванням теоретичних і прикладних досліджень з цієї проблематики. У статті автори мають на меті розглянути теоретичні аспекти деструктивного інформаційного впливу, визначити пріоритетні напрями його використання російською федерацією в ході інформаційної війни проти України. Відповідно до мети в процесі розкриття обраної теми використано наукові методи сучасної гносеології. Методологічну основу дослідження склала теорія пізнання явищ як концептуальних положень,

[27] Doctor of Science in Law, Associate Professor, Vice-rector for scientific work, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[28] Ph.D (Law), Security Service of Ukraine, Kyiv, Ukraine.
[29] Ph.D (Law), Security Service of Ukraine, Kyiv, Ukraine.
[30] Ph.D (Law), National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[31] Security Service of Ukraine, Kyiv, Ukraine.

informational influence on Ukraine and the most vulnerable areas in information space of the country.

Key words: information security, destructive informational influence, special information operations, national security of Ukraine, democratic society, cyberterrorism.

розроблених фахівцями та експертами у сфері інформаційної безпеки. Застосовано також діалектичний, загально-логічний, порівняльний, функціональний, системний та інші методи. Результати аналізу теоретичних напрацювань вітчизняних та іноземних науковців і дослідників дозволили визначити пріоритетні для противника напрями використання деструктивного інформаційного впливу щодо України та найбільш уразливі місця інформаційного простору держави.

Ключові слова: інформаційна безпека, деструктивний інформаційний вплив, спеціальні інформаційні операції, національна безпека України, демократичне суспільство, кібертероризм.

Introduction

The great power rivalry to possess the information resource in a world-wide spectrum space is becoming an arena of a fierce geopolitical strategic competition, an effective tool to influence and enhance the international community, public opinion and state national security.

The analysis in the sphere of secure national security indicates that in spite of using current military operations, the enemy disseminates controversial information using electronic, social and other networks to achieve its strategic and tactical goals. Such networks can be used to withhold political, economic, and psychological enforcement and malicious distortion of the citizens' critical perception.

Fundamentals of the destruction of the decent governance and psyche destruction of world society membership are generated into the process of implementing destructive informational influence.

Theoretical knowledge and practical application in spheres of policy, economy, military, special services and law enforcement agencies are used in the drafting of special information operations. For this reason, advanced technologies and psychological techniques can be applied in combination with specific capabilities of security and defense forces and can cause a significant response in the society.

The implementation of such actions and operations can lead to destabilization of the political situation in a particular region and state; can discredit a country on the international level. Furthermore, it can lead to the emergence of social tension and conflicts, military defeats on local and global scale. In long term perspectives it can lead to a gradual change of public consciousness, distortion of the national ideology, loss of national identity, and can be evoked with biased and malicious memories. It should be pointed out that in short- and long-term perspectives, the issues of changing political, economic, military, scientific and other elites can be decided simultaneously.

The organized systematic and comprehensive disinformation by Russian law enforcement bodies is an urgent and high priority threat to Ukraine sovereignty and territorial integrity. The above-mentioned study requires the normative legal regulation improvement of the information dissemination, the procedure of information access restriction in cases of false information; methodology and legal research to bring to justice the agents involved in the information dissemination.

Ukraine has faced a number of challenges and threats caused by the destructive informational influence. In particular, they are the complex of critical perception of the information, the growing public distrust to news and media, declining trust in democratic institutions, ruling elite, Armed Forces of Ukraine and law enforcement agencies, etc.

The destructive informational influence that accompanies external armed aggression and takes place in the internal information space of Ukraine has goals to strengthen anti-Ukrainian positions through targeted pressure on state agencies, to enhance society polarization and to substitute traditional national values. In the

context of counteracting such an influence, there is a dispute in relation to the limits of state intervention in the information sphere. Meanwhile the democracy can exist only if media are strong and independent; the guarantee of the rights to freedom of speech and expression; the adherence to democratic principles in the context of weapons escalation of the so-called "mass information destruction".

The issue of countering destructive informational influence, systematic disinformation is discussed at the national and global levels with the participation of representatives of international institutions and profound experts. Such approach is quite effective, especially for so-called "young" democratic countries.

Our analysis of law enforcement practices to ensure information security as an element of national security in the European Union gives a ground to believe that a unified model of developing an international security system is lacking. (Svitlana, Onyshchuk, Onyshchuk & Chernysh, 2020; Vlasenko, Chernysh, Dergach, Lobunets & Kurylo, 2020; Chernysh, Pogrebnaya, Montrin, Koval & Paramonova, 2020; Chernysh, Prozorov, Tytarenko, Matsiuk & Lebedev, 2022).

Given the above mentioned, there is a fundamental principle for a comprehensive generalization of previously developed theoretical researched issues and modeling of the effective system of counteraction to destructive informational influence.

Methods of the research

A polymethodological approach was used for the research. It covers the following groups of methods: general philosophical (dialectical, phenomenological, axiological, hermeneutic, anthropological, synergistic, etc.); general scientific (abstraction, analysis and synthesis, system analysis, etc.); special (questionnaires, content analysis, deontic, etc.); legal (historical-legal, comparative-legal, formal-dogmatic, etc.). In particular, with the help of the dialectical method, the environment of destructive information influence was investigated, its numerous connections with social processes, dependence on socio-economic, political, international and other factors were traced. Using the hermeneutic method, the meaning of the main categories used in the field of information relations was determined. The methods of analysis and synthesis were used to clarify the content of the institution of the implementation of destructive information influence, as a component of the subject of ensuring the state security of Ukraine. The system-structural approach became the basis of the analysis of various tools, methods and means of destructive information influence in their relationship.

Results and discussion

Considering the rapid process of information and communication technologies development, outstanding scientists draw the attention to the information research use in vital areas of public life.

Information is one of the core elements of the interaction between the individual and the state. In the matter of armed conflict, it becomes an important tool for conducting "hybrid warfare", which performs public opinion and acts as a booster of protest potential.

Nowadays, the multi-spectral approach of the information sphere cannot be regarded without informational influence, as well as destructive nature. Its implementation by the opposing side is caused by the requirement to achieve certain goals in short- or long-term prospects.

Since the proclamation of independence of Ukraine, a rapid evolution from total control to democracy has begun. However, in spite of positive changes, serious negative impacts have arisen. Such changes produce threats to national sovereignty, territorial integrity of Ukraine and other elements of national security. External armed aggression boosted these acts.

The result of the enemy deliberate destructive influence on citizens' consciousness and subconsciousness is the support of aggression by individuals, motivation to commit acts of disobedience and other illegal actions. At the same time, Ukrainians who have free access to essential information resources, due to some activities and lack of some knowledge how to use information technologies, haven't become aware about destructive informational influence as an element of information warfare and the information flow from different sources.

It was German psychologist and psychoanalyst E. Fromm who first introduced the concept "destructiveness" in the scientific terminology as a malignant form of aggression and destruction. In his research, he argued that "destructiveness is not an innate human instinct; it is the duty that is born by an individual" (Fromm, 2019). According to the E. Fromm's theory, it should be

stated that destructiveness is not only the duty that is born by an individual, but also the duty that is used by an individual at personal and social levels with the aim of informational influence.

The traditional aspects of destructive informational influence are: ideological and psychological environment in society; resources that disclose spiritual, cultural, historical and other values, state and nation achievements in different spheres; information infrastructure; systems that form public consciousness and public opinion; the system of development and adoption of political decisions; human consciousness and behavior (Petryk, 2009). In the process of implementing destructive informational influence, some aspects are also added, which are: specific target audience, the psyche of the political elites and population of the confronted states, administrative decision-making process in the field of national security.

The main priorities of destructive informational influence are: manipulation of public consciousness and state political orientation; social destabilization; the conflict of interests between public authorities; the conflict of social, political, national-ethnic and religious-confessional groups; discrediting facts of the historical and national identity; changing worldviews and values; creating a spiritual atmosphere; undermining international state authority; formation of preconditions for economic, military or spiritual defeat; undermining morale and psychological stability of the population; defense capability and combat state potential.

Taking into account the activities of special services during warfare, it is also advisable to blend in national special services activities and law enforcement agencies to the sphere of destructive informational influence and leveling the results achieved by them.

Nowadays, such influence is widely produced by the aggressor during information warfare, which is a kind of hostilities, tools and methods of information processing that are applied as a kind of weapons, allowing deliberately, quickly and secretly to influence military and civilian information systems in order to undermine policy, economy, combat capability, and the information element of state security.

Acts of destructive informational influence as an element of information warfare can target a wide range of public relations and vital areas of national security (policy, economy, military and defense spheres, and science, etc.).

Originally, the term “information warfare” was used in 1920 by British Historian J. Fuller who analyzed the origin of the First World War. The term was adopted by Americans. In 1966, A. Dulles in his book “Secret Surrender” used this term to define a special type of Intelligence Special Operations (Dulles, 1966). In 1976, the term “information warfare” was used by a future adviser to the Department of Defense and the White House during the presidencies of R. Reagan and J. Bush, a physicist T. Ron in the report “Weapons Systems and Information Warfare”. He stated that the information element is an integral element of the American economy and can be a vulnerable target in peacetime or wartime and has defined the sphere and the role of the information element in the processes of escalating the Cold War. In the document, T. Ron outlined his concept of information warfare’s, acquiring the idea of “reducing the information flow of the enemy and, instead, protecting or improving its own one”. Moreover, he emphasized that the dissemination speed in the information warfare is a decisive element for victory. In this sense, all world countries, without exception, are vulnerable. The USA can also be a target of any information attack, and its adversaries can convince the American public of “their truth” by media manipulation (Ron, 1976).

Taking into account the conclusion of the American researcher, the concept of information warfare, “reducing the information flow of the enemy and, instead, protecting or improving its own one” should be enhanced with the idea of information flow diversion to enemy's allies. Moreover, it is to be observed that such allies may take an active or passive role in the information confrontation and change it depending on the state and trends in the development of the operational situation, in particular, with the increase or decrease in the “degree” of their own interests.

Ukrainian researchers, considering the concept “information warfare”, have not agreed on the formation of the unified approach to it yet. This is due to a certain “obsolescence” of some views on the genesis of information warfare, which has become a dynamic phenomenon in the context of information technology.

M. Libicki in the book “What is information warfare?”, which is considered to be an orthodox one among scholars, defined seven forms of information warfare, focused his attention on

revealing their manifestation depending on warfare activities, in particular:

1. Command and control (command-and-control – C2W) a military strategy that implements information warfare on the battlefield and combines physical destruction.
2. Military Intelligence (intelligence-based warfare IBW) is the collecting of critical and protecting personal information.
3. Electronic warfare (EW) is aimed against electronic communications: radio communications, television networks, computer networks, radars.
4. Psychological warfare (PSYW) covers the use of information against the human mind.
5. Hacker warfare is subversion against the enemy by creating special programs, attacks on computer networks.
6. Economic information warfare (EIW) has two forms: information blockade with limited access to information by one state to another and informational one.
7. Cyber warfare is carried out in the form of information terrorism, semantic attacks, simulated wars, Gibson's wars (warfare in the virtual space using intelligence (Libicki, 1995).

Taking into account the author's argument, a destructive information impact on consciousness can be carried out with the implementation of any information warfare forms.

Nevertheless, M. Libicki does not focus attention on determining the role of special services (intelligence and counterintelligence) in the implementation of information warfare forms. Nowadays, the background of the operational situation at the global and regional levels and the trends in its development give grounds to determ the eighth form of such a war – conducting special information operations by special services. Such operations involve the confidentiality of their organization and the comprehensive use of available means.

According to scientific theories, destructive informational impact can be carried out during information warfare or even before the beginning of it. In particular, as O. Sviderska states, even before the full-scale invasion, there was a "swaying" of the emotional and psychological state of Ukrainians. Ukraine has constantly suffered from cyber-attacks: numerous fakes, propaganda, disinformation, information attacks, attacks on the government websites, pseudo-mining of railway stations, schools and supermarkets, reports of possible full-scale interference on the territory of the state. All these facts disclose signs of strategic psychological special operations, main goals of which are to destabilize and disorient Ukrainian society, to spread hostility and panic, to force the country to make concessions to the aggressor (Sviderska O., 2018).

The term "psychological operation" (Psychological Operations, PSYOPS) emerged after the Second World War. It was grounded on the psychological impact on the leadership, population and personnel of the armed forces of foreign states. PSYOPS is aimed to change the behavior of the target audience in order to reduce the moral potential and psychological stability of the enemy before the beginning of the warfare and thereby to achieve the results of their own military and special operations. One of the main PSYOPS application in modern conditions is to ensure citizen loyalty to the occupying army, the functioning of the established regime to the temporary administration (Department of the Army, 2003).

The consequences of informational and psychological influences may spread in a while. The concept of Effects-Based-Operations is grounded on it. The main elements of it are effects of the first, second, third and further orders. Human consciousness is determined to perceive only immediate consequences, and they can be distant in time. The essence of the concept is set out in the sequence – "mechanism", "action", "effect". The final stage is the effect that will be formed by the informational and psychological impact.

Some experts in the sphere of information warfare consider that the term "psychological operation" does not correspond to the modern level of communication development. In particular, essential elements of the strategy for achieving information dominance are information management and information operations (Alberts, Garstka, Hayes & Signori, 2001).

In June 2010, the US Secretary of Defense approved to replace the term "Psychological Operations" (PSYOP) with the term "Military Information Support Operations" (MISO). It means "Military Information Support Operations" or "Information Support Operations of the Armed Forces". The initiation of the new term, according to the US military command, means "a complete substitution of doctrine, its structure and practical activity" regarding the

implementation of information operations, their transformation into the most powerful instrument of state policy (MISO, 2010).

Destructive informational impact includes an entity and an individual. During military actions, at first, entities will be the states participating in them. State agencies are interested in forming the "right" public opinion in their country and other ones. Any informational influence during armed clashes is always controlled by the state, as it has the most reliable information about territorial conflicts. As mentioned, opposing sides do not always have reliable and verified information in the conflict zone, because measures can be taken from both sides to hide applicable and relevant data and enemy disinformation as well.

The individual of destructive informational influence is a person, society and state, such groups for the protection of which or against it is targeted.

Today's reality demonstrates that ten-year war in Ukraine, economic instability, a huge amount of data do not always authorize to analyze information spreading by different sources. Information itself determines the society movement direction as a whole. The developing of the democracy and the implementation of reforms depend on how people will be able to "filter" information and adhere to "information hygiene". Unless, the "critical" part of the population using positive changes (medical, educational, economic, military reforms, as well as reforms of special services and law enforcement agencies) can be quite easily discredited on the initiative of the interested side (external aggressor, internal destabilizing forces).

Nowadays, it is not easy for an ordinary citizen to analyze a large amount of open-source information, which is due to its amount, inconsistency, and fake news, lack of official comments and distrust of state agencies. The above mentioned stated, that under the influence of fear and stress, which affect sensitivity to information valence, there is a tendency to spread information viruses as soon as possible and to carry out destructive informational influence.

Information, spread among the population, can change trends, determine state policy and radically change the attitude towards certain groups within society in countries with "new democracies" that haven`t been formed by the beginning of the digital era.

As mentioned, the destructive informational influence quite often is carried out in the process of information terrorism. Terrorist activity as one of the means to achieve illegal goals has been widely used since ancient times. However, since the 90s of the 20th century, it has been evolved significantly, which is not least due to scientific and technological progress. At the same time, terrorist activity has been integrated into information space (cybersphere), and information space, under the condition of fierce international rivalry, has become the main field of clashes and struggles of multi-vector states national interests.

Given the above mentioned, scientists and scholars pay great attention to information terrorism as a new type of terrorist acts that targets information technologies and means of communication to disrupt the functioning or destruct state infrastructure. Despite numerous scientific research and academic events devoted to information terrorism, there is no unified approach of the definition "information terrorism". In modern legal science the concept "information offenses" hasn't been formed and, moreover, any scientific approaches on effective counteraction to them haven't been developed.

The mentioned issue has become vital with "hybrid warfare" against Ukraine started by the Russian Federation. Thus, before warfare in Ukraine started, the Information Security Center of the Federal Security Service (FSB) of the Russian Federation had more than 800 employees, and the Department of Information Restriction conducting informational operations in the Donbas, consists of 60 employees.

Besides limited access to information provided against Ukraine, cyber warfare has also been taken. According to the Ukrainian CyberAlliance's speaker, Russian hackers are administered by the FSB and the President of the Russian Federation. Moreover, there is a confirmation of strong ties between Russian state agencies and well-known cybercriminals that afford extra opportunities for their security services (Demyanenko, 2017).

According to experts' results, the evolution of effective ways to counteract destructive informational influence and the effectiveness of implementation lag behind the needs of law enforcement practice and require the depth of scientific research, including empiriocriticism.

Information terrorism is an element of terrorist activity, using modern information technologies

(Internet, social networks and social messengers), carries out destructive informational influence in order to impede the functioning of state agencies.

Information terrorism includes psychological terrorism and cyberterrorism.

Psychological terrorism takes political, philosophical, legal, aesthetic, religious and other spheres.

Cyberterrorism (electronic terrorism) is a kind of terrorist act in information space. It includes deliberate and large-scale attacks to create computer malfunction using computer viruses, etc., planned and coordinated terrorist actions in cyberspace, and use the latest achievements of science and technology in the sphere of information technologies.

The main feature of modern terrorism is the dynamic use of information and psychological technologies to influence human consciousness and public opinion applying global communications. Taking into account the achievements in the information era and the functioning of global media, terrorists have made television and cyberspace their main means of influence.

Such technologies are quite often aimed at discrediting actions of top military leaders of Ukraine at the international level. Thus, the Ministry of Defense of the Russian Federation, conducting a special information operation, used targeted measures to disrupt the mission of the IAEA at Zaporizhzhya NPP.

In particular, on the eve of the arrival mission at the nuclear power plant, Russian news reported on the alleged destruction of the "Ukrainian landing force" that landed in the occupied Enerhodar. As a kind of "evidence", the Russian Defense Ministry published a story about how Ka-52 helicopters using missiles "Vikhr" destroyed a barge with military men of the Ukrainian Armed Forces during the Dnieper River crossing.

Debunking this fake, the Center for Strategic Communications and Information Security reported that Russians hit the bridge near Enerhodar. Russian TV broadcasted events of destroying a "barge with a Ukrainian landing force" near ZNPP. But in fact, they just shelled the bridge (Sitnikova, 2022).

The above mentioned activities of information terrorism demonstrates its vitality, ability to respond quickly to counter-terrorism measures and choose vulnerable spheres to ruin public life.

The key issue in the context of organizing effective counteraction to information terrorism in Ukraine is spotting and blocking separatist Internet networks used by representatives of terrorist organizations and quasi-formations on the territory of the state. They act in interests of ideology and call for the constitutional overthrow in Ukraine, violation of the territorial integrity, extremism and terrorism.

Grounded theory offers specific strategies for improving effectiveness of network security targeted by terrorists:

- targeted use of the provisions of the Council of Europe Convention on Cybercrime on the procedure for sending requests for mutual assistance in the absence of relevant international agreements, as well as norms of legislation on combating terrorism and cyberterrorism (provisions of the Council of Europe Convention on the Prevention of Terrorism, relating to public incitement to commit a terrorist crime);
- imposing strict legal liability as a deterrent factor for individuals involved in the preparation and implementation of terrorist acts;
- improving the network protection in order to prevent hackers from accessing its vulnerable components;
- cyberspace analysis to identify and analyze real and potential threats;
- exchanging of intelligence data used for terrorist aims to counteract threats in cyberspace;
- limited public coverage of successful cyber-terrorist attacks.

Thus, the effectiveness of counteracting destructive informational influence, acquirng modern information technologies, depends on the speed of implementation of international experience in legal regulation methods in the information sphere and the level of law enforcement strategies in the fight against the negative phenomenon, as well as the scientific and technical support that carries out appropriate countermeasures.

Conclusions

Innovation process in the information sphere, ways of counteracting destructive informational

influence are being discussed by scientists and scholars. Scientific ideas are under the influence of geopolitical changes and the rapid development of modern information technologies are in a constant search for better solutions. Determining such ways, the prime concern is to observe an applicable balance between principles of the democratic society functioning and limits and severity of punishment committed in this field.

Profound experts of international institutions take an active part in the discussion of key issues of counteracting such influence, systemic disinformation and preventing the use of information space for terrorist aims. Such approach is quite relevant for countries of the so-called “young” democracy, including Ukraine.

Grounded theory has a second judgement. In the preparation of identifying destructive informational influence and special information operations, some relevant theoretical and practical knowledge in the field of foreign and domestic policy, economic, military and defense spheres, as well as in the field of state security can be applied. It is a relevant case study, so problem-solving strategies and psychological techniques are developed and implemented. Commonly with specific capabilities of law enforcement agencies, they can cause a significant public opinion and assist military defeats at strategic and tactical levels.

Large-scale and dynamic transformations in the information sphere as to information warfare against Ukraine are characterized the targeted use of destructive informational influence by the aggressor. Such influence is followed by the enemy conducting special information operations and using military forces. The effects of actions can violate territorial integrity and state sovereignty, security and defense and, in general, elements of national security in Ukraine. In addition, the aggressor focuses its efforts on undermining international image of Ukraine, good-neighbourly relations and friendly cooperation in industries (agricultural, metallurgical and mining, defense-industrial, transport industries) at local and global markets, and compromising achievements in IT technologies.

Information space of Ukraine suffers from significant threats. Vulnerable places of domestic information space are the national idea, culture, scientific achievements, public opinion and consciousness, the attitude towards friendly neighboring countries and media.

Destructive informational influence on Ukraine can be carried out by the aggressor (enemy), its allies and local quasi-formations. An integrated approach can be applied. Such approach can also be multi-vector (involve several areas of application: policy, economy, media, etc.) and one-vector (security and defense spheres).

Nowadays, Ukraine together with global communities is taking active measures to counteract such negative phenomenon in all vital spheres of life ensuring national security of the state. At the same time, ways to increase the effectiveness of the fight against the aggressor in information space are the interchange in research of scientific and practical application, comprehensive analysis, methodological and technological assistance of those who involved in counteracting governmental institutions.

Bibliographic references

Alberts, D., Garstka, J., Hayes, R., & Signori, D. (2001) Understanding Information Age Warfare. CCRP Publication Series. URL: http://www.dodccrp.org/files/Alberts_UIAW.pdf

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

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

Demyanenko, M. (2017) NATO's experience in creating an effective information and psychological combat system. Resonance, 23, pp. 3-17. URL: http://nbuviap.gov.ua/images/rezonans/2017/rez23.pdf (In Ukranian)

Department of the Army (2003) Psychological Operations Tactics, Techniques, and Procedures. URL: https://irp.fas.org/doddir/army/fm3-05-301.pdf

Dulles, A. (1966). The Secret Surrender. Harper & Row. URL: https://books.google.de/books/about/The_Secret_Surrender.html?id=b3kNAAAAIAAJ&redir_esc=y

Fromm, E. (2019). Escape from freedom / Erich

Fromm; translation from English M. Yakovlev. Kharkiv: Book Club «Family Leisure Club», 288 p. URL: https://chtyvo.org.ua/authors/Fromm_Erich/Vtecha_vid_svobody/

Libicki, M. (1995) What is information warfare? Washington: National Defense University Press, 104 p. URL: http://www.dodccrp.org/files/Libicki_What_Is.pdf

MISO (2010). Military Information Support Operations. URL: https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf

Petryk, V. (2009). The essence of information security of the state, society and the individual. Legal magazine, 5. URL: http://www.justinian.com.ua/article.php?id=3222. (In Ukranian)

Ron, T. (1976). Weapon Systems and Information War. Boeing Aerospace Co. Seattle: WA. URL: https://acortar.link/78jebT

Sitnikova, I. (2022). In russia, they showed a story about the destruction of the «barge with the Ukrainian landing party» near the ZNPP. But actually they fired at the bridge support. Hromadske. URL: https://acortar.link/xczMN9 (In Ukranian)

Sviderska, O. (2018). Digital propaganda and information security risks in the context of the Russian-Ukrainian war. Scientific magazine «Politician». URL: http://politicus.od.ua/ (In Ukranian)

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

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, VIII(2), pp. 200-209.