UDC 32.019.5

I. Vashchenko

E. Poltavskyi

THEORY AND PRACTICE OF CONDUCTING SPECIAL INFORMATION OPERATIONS IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

The article analyses the role and place of information wars in the modern world political process. The peculiarities of the russian-Ukrainian information warfare are studied. The algorithm of actions during special information operations is considered, where propaganda and psychological work is carried out to directly influence the consciousness and behaviour of any audience in order to achieve political or military goals.

Keywords: *disinformation, mass media, information warfare, information and psychological operation, information influence, communication technologies, manipulation, national security system, world community, psychological operation, propaganda, fake.*

Statement of the problem. The development of the global information space and technologies, the specifics of the social, economic, and political conditions of the modern world community actively influence the peculiarities of armed conflicts. Today, the vast majority of leading states consider the influence of information on their adversaries as one of the most effective tools for implementing their foreign policy, which allows them to exert intense pressure at all levels of state and social structure in any region of the world. Such challenges require the creation of a specific national security system.

Scholars argue that in the future world, leadership will be determined by the ability of states to control the information space. Currently, the key role is played by the media, Internet channels, and information flow control systems. Therefore, it is no coincidence that in the process of forming a new world order, the leading states are taking decisive steps to make a breakthrough in the information sphere.

The discrepancy between the objective need to create an effective system of countering information influence operations and the low level of readiness of civil society to resist attempts to manipulate the consciousness of its members remains a pressing issue. The mass consciousness of citizens has not yet fully formed an understanding of the threat posed by modern communication technologies, especially if their hidden aggression is used for political purposes [1].

Today, the information aggression of the russian federation against Ukraine includes a group of tools that use destructive information methods of influence and are aimed at the system of public administration, the internal division of Ukrainian society through the intensive use of disorienting, disorganising, disinforming, destabilising factors.

Analysis of recent research and publications. The problem of modern information wars has been studied by both foreign and domestic scholars.

The peculiarities of modern information warfare in the online space were described by researcher O. Kurban [2]. The collective monograph (edited by V. Horbulin) thoroughly investigated the essence of hybrid warfare as a new type of global confrontation. The researchers examined in detail the peculiarities of hybrid warfare in various dimensions: military, political, economic, social, humanitarian, and information [3]. Y. Horban analysed the phenomenon of information warfare in detail and described the means of its conduct [4]. The issue of the need to ensure the information security of the state as a result of the spread of information threats was raised by Y. Chmyr [5]. A team of authors led by V. Smolianiuk revealed technological methods of influencing political processes in order to obtain the desired results, and also studied the dependence of democratic politics on technological saturation, which has both positive and negative consequences for the political system and society [6].

However, this topic has been insufficiently studied in terms of the introduction of new methods of deploying information aggression against Ukraine. The russian-Ukrainian war generates new forms of information influence, which constantly attracts the attention of researchers and encourages further study.

The purpose of the article is to analyse the term "information warfare", to explore the methods and features of the Russian-Ukrainian information warfare, and to reveal the role of the latest information and communication technologies as a weapon of modern armed conflicts used by technologically advanced states in the struggle for world leadership.

Summary of the main material. Human civilisation has always been subject to information influence at all levels, and any military victory over the enemy already indicated the fact of defeat in the information war. With the help of information, it was possible to observe the course of hostilities, analyse events, and communicate the necessary information to subordinates. The emergence of information systems became an integral part of socio-political life and the beginning of fundamental changes in the methods of warfare, which were already supported by a large amount of information. With the development of information technology, the methods of successful combat operations are also being improved, making it possible to manipulate enemy information.

The following definition can be given: information warfare is a communication technology of influencing the enemy's information systems in order to achieve information superiority in the interests of national strategy while protecting one's own information. Thus, information warfare is a key tool used to conduct a strategic attack on the enemy.

The history of this term dates back to the 70s of the twentieth century, when A. Dallas' book "Secret Surrender" (1967) was published. This phrase was used as the name of a special type of intelligence special operations. The term "information warfare" was used in 1976 by T. Rona in his report "Weapons Systems and Information Warfare", in which he stressed that information infrastructure was becoming a key component of the American economy, a vulnerable target even in peacetime.

The term "information warfare" came into active use at the end of the 20th century after the end of the Cold War. Subsequently, military theorists based armed conflicts on the division of the entire theatre of operations into two components: traditional space and cyberspace, where the latter is more important for neutralising the enemy's armed forces [7].

Thus, the traditional spheres of warfare, in addition to land, sea, air and space, include the information sphere, where the main targets are the information structure of the state and the enemy's psyche. The struggle for leadership in the global political process is gradually shifting to the information environment.

The information environment is a set of individuals, organisations and systems that collect, process and disseminate information. It includes three dimensions.

The physical dimension is a control system that enables information operations in the air, on land, at sea and in space. It includes communication networks and the infrastructure of the state.

The information dimension is the environment where information is collected, processed, stored, and disseminated. It includes all information flows.

The cognitive dimension is the consciousness and environment of decision makers (their emotions, awareness, understanding).

Information warfare is conducted on two levels.

1. State. The goal of information warfare is to weaken the positions of competing states, disrupt the system of public administration through information influence on the political, diplomatic, economic and social spheres, as well as through psychological operations and subversive propaganda.

2. Military. The purpose of information warfare is to achieve information superiority by influencing the enemy's information and information systems while protecting its own information and information systems.

Later, military theorists defined the concept of "information warfare" as follows. *Information warfare is a* set of information operations aimed at the enemy's system of state and military governance, which in peacetime leads to decisions favourable to the initiator of information influence, and in the course of an armed conflict completely neutralises the operation of the enemy's governance infrastructure [8].

As military practice has shown, information warfare is not accidental; it involves coordinated activities to use information both on the real battlefield and in the economic, political and social spheres.

Gradually, the military and political leadership of the leading states began to prefer the term "information operation" in official documents.

An information operation is a comprehensive use of electronic warfare, computer network operations,

psychological operations, military disinformation operations and security operations to influence the enemy's decision-making process while protecting its own information and information systems.

Information operations primarily involve influencing decisions and the decision-making process. The strategic goal of information operations is to deter a potential adversary from actions that threaten the national interests of the state.

The main activities of the information operation are extremely diverse and cover the following areas.

1. Infrastructure for the life of the state. There is a distinction between production infrastructure (roads, canals, ports, warehouses, communication systems) and social infrastructure (schools, hospitals, libraries, theatres). Sometimes this term is used to refer to a set of infrastructure sectors of the economy (telecommunications, transport networks, power plants, banking systems, communications, education, healthcare).

2. Industrial espionage. It is aimed at stealing patented information, gaining a competitive advantage by ousting a rival, and destroying important data.

3. Hacking of personal passwords of VIPs, identification numbers, bank accounts.

4. EElectronic interference in the management of military facilities, disabling military communications systems.

5. The global computer network Internet.

Thus, it can be emphasised that information warfare is a new form of conflict where direct attacks on information systems are carried out to influence the enemy with the aim of its further destruction [9].

The components of an information operation include the following.

1. A psychological operation involves measures to disseminate specially prepared information in order to influence the emotional state, motivation and reasoning of actions, decision-making and behaviour of individual leaders, organisations, social or national groups in a direction favourable to the aggressor country.

2. Disinformation is a method of psychological influence, which consists in providing the object with false or distorted information that misleads it about the true state of affairs and creates a distorted reality. As a rule, groups of people are the targets of psychological operations, while disinformation is targeted at individuals.

3. Electronic warfare prevents the enemy from obtaining accurate information, including electronic suppression and electronic defence. Electronic warfare has become one of the most important areas of the Russian-Ukrainian war, where the parties are forced to constantly improve their technologies and techniques that affect the intensity of hostilities.

4. Network security covers computer network attacks, protection and use of enemy computer networks for own purposes.

5. Information security involves measures to protect information and information systems by ensuring their integrity, confidentiality and authenticity.

6. Physical security is aimed at protecting personnel who have access to information systems, preventing unauthorised access to equipment, and protecting documents from espionage, damage, and theft.

7. Information attack is a targeted action with the use of hardware and software tools to breach the information security of a system, which allows to influence its content.

8. A physical attack is aimed at the enemy's control system in order to affect its ability to control the target audience.

9. Counterintelligence involves the collection of information or activities aimed at protecting against espionage, assassinations ordered on behalf of foreign governments, organisations or terrorist groups.

It should be noted that the auxiliary components of an information operation do not always have a military purpose, but they operate in the information environment to influence the enemy's information capabilities [10].

Domestic scholars emphasise that the main task of information operations is to manipulate the mass consciousness aimed at the following:

– introduction of hostile ideas and views into the public consciousness and the minds of individual citizens;

– disorientation of society and its disinformation;

– weakening of statehood beliefs and intimidation of the population;

– control of the enemy's information space and protection of the information functions of the national armed forces from hostile actions.

A review of the material presented here convincingly proves that the information aggression of the russian federation against Ukraine was not accidental and was not only a violation of existing international law, but also a concerted effort to use information weapons to conduct real hostilities. Information influence is carried out in various areas, usually in the spheres of state activity [11].

ArmyInform's correspondents note that people absorb information that already exists in their minds better, so any propaganda campaign is aimed at the "resonance effect", where information is used to change the behaviour

of the audience. Usually, such information is disguised as knowledge and stereotypes that already exist in the minds of a particular social group. In such circumstances, the effectiveness of information influence is achieved by giving an artificially exaggerated importance to a fact or problem, which gradually begins to destroy the existing system of values and moral norms of behaviour that regulate social relations [12].

Military experts point out that the impact on information systems through specially prepared operations creates an information advantage that allows not only to collect, process, and distribute the entire flow of information events, but also to act ahead of the enemy in its response.

Classical definitions of information and psychological operations (IPO) include planned actions to convey specific information to foreign audiences in order to influence their feelings, motives, critical thinking, and the activities of foreign governments, organisations, groups, or individuals.

The definition of IPSO is officially enshrined in the US Army Field Manual, where psychological operations constitute a component of national power that directly influences the national will of friendly, neutral, and hostile forces and societies. It is achieved by influencing the attitudes and actions of groups that are the targets of psychological operations to persuade them to support national policies and national goals.

The russian aggressor is actively using IWOT against Ukraine in order to create favourable conditions for controlling the territory and to do everything possible to prevent Ukrainians from resisting russian troops. Common elements of IPSO include propaganda, information manipulation and cyberattacks, where elements may be based on real events.

Thus, the definition of "information and psychological operations" is only a terminologically disguised propaganda of a covert operation conducted with the help of specially trained services [13].

The conclusions of the US Institute for National Strategic Studies emphasise that a key role in the implementation of an information operation is played by a psychological operation, where planned propaganda and psychological work is designed for any audience in order to influence its behaviour in order to achieve political and military goals. In wide circles of military theorists, a covert destructive operation conducted by special services to weaken the state and social order is called a special information operation.

Special information operations are planned actions aimed at hostile, friendly or neutral audiences, which involve influencing their consciousness and behaviour through the use of organised information and information technology to achieve a goal. This operation is carried out at the macro and micro levels.

The macro level defines that advocacy work is focused on specific social groups and is carried out mainly through the media and communication channels.

The micro-level involves ideological propaganda work, which is personalised and carried out through interpersonal communication. For this purpose, activities aimed at spreading rumours and inciting the population of the state to negative behaviour are used [14].

In order to create a favourable political, ideological, social and economic environment during a special information operation, intelligence services *use* well-known methods of *disinformation to* exert covert information influence, which involve misleading the target about the authenticity of intentions and encourage actions programmed by the aggressor. The main disinformation tools are as follows.

1. Forgery of *documents* is an important tool for spreading false information. Destructive influences, negative narratives, distortions of official statements of the Ministry of Defence of Ukraine, personal letters of Ukrainian officials are common in the practice of pro-russian information resources aimed at misinforming society. For example, a fake report by the Security Service of Ukraine on the facts of systematic violations of international law by Ukrainian military personnel and their responsibility for the crimes committed.

2. The *paid-for articles in the local and foreign press* have clearly defined recipients, and agents of influence in the circles of journalists, public figures and advertising resources are used to disseminate such articles in the media space of foreign countries.

3. The *use of third-country media* to get disinformation into the information space, where Internet publications that have formal ties to the state are actively used. The factors that contribute to the spread of fakes include: low level of public awareness of the issues under discussion; lack of such materials in search engines regarding their reliability; the ability of the civilian population to perceive shock news, which is higher than the ability to perceive ordinary news; public distrust of expertise; excess of information on the Internet; development of leak-based journalism [15].

Markers of manipulation in the press and online media include the following:

– use of information sources that cannot be verified;

– an artificial combination of unrelated events in one material;

– emotional colouring of words used to describe people and phenomena;
– categorical judgements that call for aggressive action.

Markers of fake news on social media include:
– newly created accounts from which information is disseminated;
– incredible, shocking information;
– wave-like spread of the message;
– lack of references to the original source.

As an example, let's look at the broadcast of a favourite topic for a russian TV channel – stories about criminal acts by members of the Ukrainian Armed Forces. The complete lie is instantly spread by the russian media and social networks, and the russian audience receives a dose of fear and hatred towards the Ukrainian army.

Manipulation solves such problems:
– introducing hostile ideas and views into the public and individual consciousness;
– disorientation and misinformation of the population;
– weakening of beliefs about existing moral standards of behaviour;
– intimidating its population with the image of the enemy;
– intimidation of the enemy with its own power and future terror for disobedience.

One of the most common methods of information influence is *propaganda.* It involves the dissemination of political, philosophical, scientific, artistic, or artistic ideas in order to control public opinion in relation to a certain situation, which is beneficial to the organisers.

A striking example of propaganda campaigns was the activity of the rashists ideologue Johannes Goebbels, who proclaimed the key principles of propaganda:

– propaganda should be large-scale and continuous, coming from several different sources at the same time, because people only learn what they have heard thousands of times;
– simplified forms of any message are perceived even by primitive individuals;
– maximum uniformity of clear, concise messages that should be repeated in each information message;
– propaganda does not provide for any differentiated approaches, does not allow for fluctuations, different options and possibilities;
– appealing to the emotions of the crowd with minimal use of rationality: you can weave ropes out of a crowd that is under emotion;
– shock and lies are the basis of effective propaganda; shocking messages must be disseminated instantly through an attractive medium and arouse the interest of the audience.

The Centre for Countering Disinformation at the National Security and Defence Council of Ukraine has studied the analogies between the propaganda approaches of the Nazi in World War II and the modern-day rashists in the war against Ukraine. It was found that the kremlin leadership is actively imitating the methods and techniques of Nazi Germany's ideologues. Today, in order to manipulate public opinion, the Russian Federation is changing the minds of its citizens with simple but large-scale lies by establishing strict state control over the media and culture. For example, the annexation of Crimea in 2014 was presented to the russian audience as a "triumph of historical justice" and "protection of russian-speaking citizens on the peninsula". An example is the documentary film by producer F. Bondarchuk "Sevastopol. russian Troy" [16].

The most popular source of information in Ukraine since the large-scale russian invasion has been the Internet, where social media users can find answers to any question. Due to the lack of editorial control, disinformation can spread very quickly. Social media, where everyone has the opportunity to create their own content, is gradually gaining popularity.

Therefore, the information-rich Internet requires citizens to be able to identify misleading sources. This should be done in the following way.

1. Check the source of information**.** Look for reputable news agencies that you can trust or official resources that provide accurate information.

2. Check the consistency of information. As a rule, disinformation contains inconsistencies, discrepancies, and contradictory details.

3. Checking the assessment of evidence. Disinformation has no evidence base, it relies on anecdotal accounts and selective reporting.

Thus, there is an urgent need to counter disinformation on the platform from which it is spread. Facebook, Google and Twitter all have their own systems that allow readers to report false information. A true story contains a lot of facts, whether through expert quotes, official statistics or eyewitness accounts.

It is important to clearly and confidently understand that disinformation remains one of the main challenges for the Ukrainian state due to its negative impact on human consciousness, public opinion, and national security. It is worth noting that in the information age, disinformation has become one of the main challenges for both individual states and the entire international community [17].

The mechanisms of *diversification of public consciousness* should be considered a threat to Ukraine's national security. It involves the diversion of the ruling elite's attention to various artificially created problems and their distraction from solving the priority tasks of socio-political and economic development. Kremlin theorists use the following forms of diversification of public consciousness against Ukraine:

– destabilisation of the socio-political situation in the country and its individual regions;

– intensification of a humiliating campaign against the political course of the state and its individual leaders in various international organisations;

– initiation of scandalous lawsuits, application of international sanctions.

This form of information attack is used to put pressure on the political leadership of the state to force it to accept the kremlin's scenario for resolving the armed conflict. In its information aggression, the russian federation focuses on the following areas:

– imposing the idea that the Ukrainian authorities are incapable of governing the state and making rational decisions;

– Creating the perception that the Ukrainian elite is more concerned with its own interests than with events on the frontlines;

– Formation of a negative assessment of the military and political leadership of the state, as chaotic hostilities lead to unjustified losses among the Ukrainian defence forces;

– spreading fake news that the Armed Forces of Ukraine are demoralised and unable to conduct organised combat operations.

The British Institute for the Study of War explains that the target audience for Kremlin theorists is the population of the russian federation itself, the russian-speaking diaspora, and citizens of Western Europe. Therefore, today, the vast majority of counterinformation measures should be taken by the state authorities and diplomatic missions with the broad support of the media.

A widespread influence of the russian federation on the Ukrainian audience is *psychological pressure,* which involves influencing the human psyche through threats, intimidation, in order to induce a planned model of behaviour. The following forms of psychological pressure are used against the Ukrainian population:

– bringing information to citizens about non-existent threats;

– predictions of future repression and persecution;

– committing terrorist acts and taking hostages.

In the information aggression against Ukraine, russian TV channels actively used 25th frame technologies with the use of manipulative technologies for information and psychological influence on viewers.

Active means of modifying public consciousness include the *spread of false rumours* – activities aimed at disseminating false information among the general population through informal channels in order to disorganise society and the state or its individual institutions. Through informal communication, people in a critical situation spontaneously unite in groups of like-minded people to explain the problem situationg and use their intellectual capabilities together.

In its information war against Ukraine, the aggressor country uses almost the entire arsenal of influence on the minds of its citizens. And, as a result, Ukrainians are seen by the average russian as "Banderites", "American puppets", and an enemy nation. Accordingly, the attitude of Ukrainians towards Russians has also changed, as such a massive information attack has never happened before [18].

During the russian-Ukrainian information war, a common scheme on social media was the creation of fake pages of Ukrainian volunteers, military personnel and journalists, where russians aim to obtain certain information, discredit the Ukrainian defence forces, disorient society and spread fake news.

Under the guise of journalists and production project organisers, pro-russian channels get to know the military to find out their personal data. Today, a significant number of TikTok accounts are disguised as the personal pages of members of the defence forces, posting real videos of Ukrainian soldiers, but with a completely different narrative. Such a clone page can have a large number of subscribers and millions of views. Criminals use photos and videos of real accounts to disguise themselves and gain the trust of users. Therefore, you need to be extremely careful not to share personal information until you are sure that you are

communicating with a real person. When you find out that you are facing a fake, you should complain about it so that the social network administration can block the malicious page [19].

In early 2024, a TikTok report reported the discovery of a large number of fake accounts spreading disinformation about the russian-Ukrainian war. According to the platform's organisers, the posts on the video-sharing site were aimed at Ukrainian, russian and European users. The russian fakes were intended to artificially reinforce pro-russian narratives about the war, with a common occurrence being false claims that high-ranking Ukrainian officials and their relatives have been buying luxury cars and villas abroad since the start of the large-scale war against Ukraine. Such video material has an obvious purpose – to stop Western support.

According to Ukrinform, the European Commission has published a report on compliance with the Code of Conduct on Disinformation, which was voluntarily joined by key international Internet platforms, including Google, Meta, Microsoft, and TikTok [20].

It should be noted that Ukraine, its state authorities, society, and the media were not fully prepared for such a massive information aggression, which is broadly referred to as a "hybrid war". Therefore, the primary task of all state, public, and scientific institutions is to develop effective measures to neutralize the information and psychological activities of the russian federation. The challenges facing Ukraine require prompt measures to modernise the country's information security system. The circumstances that have developed in the field of information security of Ukrainian society after the large-scale aggression of the russian federation have become a real threat to the existence of Ukrainian statehood.

It should be added that when analysing the state of information security, political, social and technical factors that directly affect the national security of the state should be taken into account. The impact of information threats on social groups results in aggravation of contradictions between different social strata, intensification of political struggle, incitement of religious and ethnic disputes, decline in the culture of the population, increase in crime and spread of inhumane ideas.

The impact of information threats on public authorities responsible for preparing and making decisions disrupts control and management, and leads to the leakage of information containing state secrets. It is worth noting that information security in the public administration system is a component of Ukraine's national security, which should ensure the protection of the public administration system from aggressive information and communication threats and the protection of citizens from information aggression.

Currently, the real threats to Ukraine's national security in the information sphere are as follows:

– The russian IPSO aims to demoralise the personnel of the Armed Forces of Ukraine, create panic, aggravate the socio-economic situation, incite national conflicts, and dominate the Ukrainian information space;

– insufficient development of the information infrastructure, which prevents Ukraine from countering information aggression and pursuing its national interests through the media space;

– ineffective state information policy, imperfect legislation and a low level of media culture;

– there is no mechanism for protecting information and providing training for public administration in the field of information security.

The frontline of the russian federation's information aggression is extremely broad: from public administration and the national security sector to ordinary citizens. The enemy uses every opportunity to harm Ukrainian statehood. The most common type of cyberattack today is emails with malware, which are aimed at destroying information systems through the mechanism of taking over credentials [21].

During the russian-Ukrainian information war, one of the priorities of the kremlin leadership is hidden information threats, which allow it to artificially create internal contradictions and purposefully control the political system from the outside. In such circumstances, a controlled political system is formed, whose behaviour can be easily predicted in real time and, through an appropriate algorithm of information influence, forced to make the desired decision**.**

Conclusions

Thus, information warfare is a form of confrontation between states in the modern world political process, which involves inflicting maximum damage to the enemy in the information environment. It is worth noting that information influence is exerted through specially prepared information operations by directly negatively affecting the public administration system to weaken its real and potential capabilities, create problems of internal development, conduct foreign policy activities, maintain international relations, and damage the political image of the state.

A widespread type of information operations today is IPSO, which involves the use of coordinated forms and methods of psychological influence. They consist of political, military, economic, diplomatic, information and psychological measures aimed at a specific person or group of people in order to introduce hostile ideological or social attitudes into their environment with the subsequent formation of false stereotypes of behaviour and directing public opinion in the desired direction.

The russian-Ukrainian information war against Ukraine uses all the elements of IWPS: disinformation, propaganda, diversification of public consciousness, psychological pressure, spreading rumours, and cyberattacks. A thorough study of these elements will allow not only to plan measures to detect, prevent, and stop negative information influence, but also to prepare for counterinformation activities.

Russian IPSO is a sophisticated system of influencing the psychological state of the Ukrainian audience, and is used to reduce the moral and psychological state through social networks and messengers. The problem of protecting information systems from negative information has never been more urgent, as targeted information influence leads to the self-destruction of the political system and the degradation of public opinion. Creating a universal defence algorithm to help detect the onset of information aggression remains a challenging task. The fight against russian IPSO requires attention and targeted measures on the part of every citizen, so it is important to develop critical thinking and analytical forecasts to distinguish objective information from manipulation and disinformation. It should be remembered that the main task of IPSO is to disturb opinions and beliefs.

Information weapons can achieve maximum effect when used against vulnerable parts of the political system, which include the decision-making system and the public administration. Therefore, in further research, it is planned to systematise the manifestations of the russian federation's information aggression during psychological pressure and diversification of public opinion in Ukraine.

References

1. Zhadko V. O. (ed.) (2018). *Hibrydna viina i zhurnalistyka. Problemy informatsiinoi bezpeky* [Hybrid war and journalism. Problems of information security]. Kyiv : NPU, 2018 [in Ukrainian].

2. Kurban O. V. (2016). *Suchasni informatsiini viiny v merezhevomu on-lain prostori* [Modern information wars in the online network space]. Kyiv : VIKNU, 2016 [in Ukrainian].

3. Horbulin V. P. (ed.) (2017). *Svitova hibrydna viina: ukrainskyi front* [Global gibryd war: the Ukrainian front]. Kyiv : Natsionalnyi instytut stratehichnykh doslidzhen, 2017 [in Ukrainian].

4. Horban Yu. O. (2015). *Informatsiina viina proty Ukrainy ta zasoby yii vedennia* [Information war against Ukraine and means of conducting it]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*, vol. 1, pp. 136–141 [in Ukrainian].

5. Chmyr Ya. I. (2018). *Problemy zabezpechennia informatsiinoi bezpeky v systemi publichnoho upravlinnia* [Promlems of ensuring information security in the public administration system]. *Aspekty publichnoho upravlinnia*. Retrieved from: http://surl.li/ubwakq (accessed 15 April 2024) [in Ukrainian].

6. Smolianiuk V. F., Bulbeniuk S. S., Maneliuk Yu. M. (2021). *Politychni tekhnolohii v suchasnykh vladnykh protsesakh* [Political technologies in modern power processes]. Kyiv : KNEU [in Ukrainian].

7. Bahlikova M. (2010). *Informatsiina viina i Ukraina* [Information war and Ukraine]. *Naukovyi visnyk Uzhhorodskoho universytetu. Seriia: politolohiia, sotsiolohiia, filosofiia*, vol. 14, pp. 158–16 [in Ukrainian].

8. Shuhaiev A. V. (2019). *Fenomen informatsiinoi viiny* [The phenomenon of information warfare]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: filolohiia. Sotsialni komunikatsii,* vol. 30 (69), no. 4–2, pp.151–156 [in Ukrainian].

9. Panchenko V. M. (2016). *Informatsiini operatsii v systemi stratehichnykh komunikatsii* [Information operations in the system of strategic communications]. *Stratehichni priorytety. Seriia: polityka,* no. 4, pp. 72–79. Retrieved from: http://surl.li/mylhnc (accessed 18 April 2024) [in Ukrainian].

10. Zaporozhets O. Yu. (2012). *Informatsiine protyborstvo u zovnishnii politytsi SSHA* [Information conflict in US foreign policy]. *Aktualni problemy mizhnarodnykh vidnosyn*, vol. 107, pp. 157–164 [in Ukrainian].

11. Horbulin V. P., Dodonov O. H., Lande D. V. (2009). *Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia* [Information operations and public security: threats, countermeasures, modeling]. Kyiv : Intertekhnolohiia, 2009 [in Ukrainian].

12. Savchenko-Halushko T. (2021). *Informatsiini ta psykholohichni operatsii derzhavy-ahresora: yak tse pratsiuie* [Information and phsychological operation to the aggressor state: how it works]. Retrieved from: http://surl.li/ptefvw (accessed 18 April 2024) [in Ukrainian].

13. Hordiienko S. (2021). *Informatsiina viina, informatsiino-psykholohichni operatsii, propahanda chy dezinformuvannia na viini?* [Information war, information and phsychological operations, propaganda or disinformation in war?]. Retrieved from: khttps://arminform.chom.ua/2021/11/04/ynformachiyni-ta-psigologichni-operachiyy-derzhavi-ahresora-yak-che-prachyuye/ (accessed 24 April 2024) [in Ukrainian].

14. Troian S. S. *Spetsialni informatsiini operatsii* [Special information operations]. *Velyka ukrainska entsyklopediia*. Retrieved from: http://surl.li/kwyptr (accessed 18 April 2024) [in Ukrainian].

15. Dubov D. V., Barovska A. V., Kazdobina Yu. K. (2020). *Destruktyvni vplyvy ta nehatyvni naratyvy: instrumenty vyiavlennia ta protydii* [Destructiv influences and negative narratives: tools for detection and countermeasures]. Kyiv : Ukrainska fundatsiia bezpekovykh studii, 2020 [in Ukrainian].

16. Tsentr protydii i dezinformatsii pry RNBO Ukrainy. (2022). *Fashyzm i rashyzm – analohii informatsiinykh viin* [Fascism and racism are analogies of information wars]. Retrieved from: http://surl.li/jdlfka (accessed 5 May 2024) [in Ukrainian].

17. Myroniuk O. (2023). *Dezinformatsiia: yak rozpiznaty ta borotysia* [Misinformation: how to recognize and combat it]. Retrieved from: https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (accessed 18 April 2024) [in Ukrainian].

18. Novytska N. B., Petryk V. M., Kudyko V. M. (2022). *Propahanda, dyversyfikatsiia hromadskoi dumky, psykholohichnyi tysk ta poshyrennia chutok yak metody vedennia spetsialnykh informatsiinykh operatsii rf proty Ukrainy* [Propaganda, diversification of public opinion, psychological pressure and the spread of rumors as methords of conducting special information operations of russion federation against Ukraine]. *Irpinskyi yurydychnyi chasopys. Seriia: pravo.* Irpin : Derzhavnyi podatkovyi universytet, vol. 2 (9), pp. 105–113 [in Ukrainian].

19. *Tiktok vyiavyv ponad 12 tysiach akauntiv, yaki poshyriuvaly rosiiski feiky* [Tiktok discovered more then 12.000 accounts thet were spreading Rassian fakes]. Retrieved from: http://surl.li/oymthj. (accessed 12 March 2024) [in Ukrainian].

20. *Rospropahanda vzialasia imituvaty ukrainskykh viiskovykh – stvoriuie feikovi akaunty i storinky-klony v sotsmerezhakh – ZMI* [Rospropaganda undertook to imitate the Ukrainian military – it creates fake accounts and clone pages in social networks – mass media]. Retrieved from: http://surl.li/agfjcz (accessed 16 March 2024) [in Ukrainian].

21. Chmyr Ya. (2022). *Suchasni problemy informatsiinoi bezpeky Ukrainy ta perspektyvni napriamy yikh vyrishennia* [Modern problems of information security of Ukraine and prospective direction of their solution]. *Naukovi pratsi Mizhrehionalnoi akademii upravlinnia personalom. Seriia: politychni nauky ta publichne upravlinnia*, vol. 2 (62), pp. 149–154. Retrieved from: http://surl.li/sejbru (accessed 6 May 2024) [in Ukrainian].

The article was submitted to the editorial office on 26.05.2024

УДК 32.019.5

І. С. Ващенко, Е. М. Полтавський

ТЕОРІЯ І ПРАКТИКА ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Проаналізовано роль і місце інформаційних війн у сучасному світовому політичному процесі. Інформаційна агресія стала новим методом ведення збройної боротьби як прагнення однієї країни нав'язати своєму суперникові політичну волю шляхом комплексу заходів інформаційного, політичного, економічного, дипломатичного, воєнного характеру без оголошення війни відповідно до міжнародного права. Саме під час формування нового світового порядку передові технологічно розвинуті країни роблять рішучі кроки в інформаційній сфері.

Досліджено особливості розгортання російсько-української інформаційної війни та доведено, що

інформаційна агресія ніколи не буває випадковим явищем. Вона може й не бути порушенням існуючого міжнародного права, але є узгодженою діяльністю у використанні інформації як зброї для ведення реальних бойових дій. Вплив на інформаційні системи за допомогою спеціально підготовлених психологічних операцій створює таку інформаційну перевагу, яка дає змогу не лише збирати, обробляти, розподіляти інформаційні потоки, але й діяти на випередження противника у його відповідних діях.

Розглянуто алгоритм дій під час проведення спеціальної інформаційної операції. Наголошено, що психологічна операція відіграє головну роль, а планова пропагандистська і психологічна робота спрямована на будь-яку аудиторію з метою безпосереднього впливу на свідомість і поведінку для досягнення політичних чи військових цілей. Задля створення сприятливої обстановки під час проведення спеціальної інформаційної операції спецслужби, здійснюючи прихований інформаційний вплив, використовують увесь арсенал впливу на свідомість громадян: дезінформування, пропаганду, диверсифікація громадської думки, психологічний тиск, поширення чуток.

Ключові слова: *дезінформація, засоби масової інформації, інформаційна війна, інформаційно-психологічна операція, інформаційний вплив, комунікаційні технології, маніпуляція, система національної безпеки, світове співтовариство, психологічна операція, пропаганда, фейк.*

Vashchenko Ihor – Candidate of History Sciences, Associate Professor, Associate Professor of the Department of Military Training of the Kharkiv National University of Internal Affairs
https://orcid.org/0000-0002-1444-7538

Poltavskyi Eduard – Candidate of Juridical Sciences, Associate Professor of the Department of Legal Support of the National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-7434-7061