

require not only substantial financial resources but also institutional capacity to ensure transparent, accountable, and efficient procurement governance.

A unified legal and procedural framework for all reconstruction contracts, regardless of funding source, is essential to reduce administrative burden, accelerate tendering, and build public and donor confidence. In this context, the adaptation of PPDS approaches may serve as a foundation for expenditure modeling, institutional readiness assessment, and the development of scientific scenarios for procurement digitalization, tailored to Ukrainian realities. The implementation of the European umbrella system ERMS in the form of DREAM encompasses the creation of a unified digital platform for coordinating, planning, financing, and monitoring reconstruction projects. The results of this study can be used to improve applied mechanisms for planning and evaluating the transparency and efficiency of public procurement, particularly in monitoring Ukraine's progress in fulfilling its European integration commitments.

Keywords: public procurement; analytical approaches; financial efficiency; post-war recovery; digital tools.

Стаття надійшла до редакції 10.10.2025

УДК 323.44:004.738

JEL Classification: D83, H83, L86

DOI: <https://doi.org/10.33111/sedu.2025.57.090.103>

Oleksandr Karpenko*

Yana Tsymbalenko**

Nataliia Savchenko***

DISINFORMATION INFILTRATION: THE PHENOMENON OF EMERGENCE AND COUNTERACTION MECHANISMS

Abstract. The article substantiates the emergence of a socio-philosophical phenomenon, namely the penetration of disinformation, and analyzes the consequences of its impact on society. Accordingly, the authors developed an original approach to the definition of the concept of «penetration of disinformation». They proposed mechanisms to counter the penetration of illegal, dangerous, harmful, false, misleading, and manipulative content into Ukraine's cyberspace. In this regard, the authors highlighted the imperfection of Ukrainian legislation, which fails to regulate tools for countering disinformation and does not provide for liability for the dissemination of false information. It is substantiated

* **Oleksandr Karpenko** — Doctor of Science in Public Administration, Full Professor, Chairman, the Department of National Economy and Public Administration, Kyiv National Economic University named after Vadym Hetman (Kyiv, Ukraine), ORCID: <https://orcid.org/0000-0002-9301-7973>, dr.karpenko@kneu.edu.ua

** **Yana Tsymbalenko** — PhD in Public Administration, Associate Professor, Doctoral student at the Department of National Economy and Public Administration, Kyiv National Economic University named after Vadym Hetman (Kyiv, Ukraine), ORCID: <https://orcid.org/0000-0003-0442-7549>, email: uprav@kpi.ua

*** **Nataliia Savchenko** — Doctor of Science in Public Administration, Senior Research Scientist, National Agency of Ukraine on Civil Service (Kyiv, Ukraine), ORCID: <https://orcid.org/0000-0002-4585-1787>, chor-na_n@ukr.net

that disinformation generates public distrust of public authorities and democratic values, posing a grave danger and causing significant damage to society as a whole. The idea that disinformation infiltration is a cause of the democratic crisis becomes a hypothesis for further theoretical and methodological research. It is emphasized that, according to European standards, disinformation is not considered illegal, and its dissemination is not prohibited by law. Additionally, producers of fake news are often directly or indirectly protected by the democratic right to freedom of speech and freedom of expression. Unfortunately, the EU countries are still fighting not disinformation, but cybercrime and the spread of illegal content related to extremism, racial hatred, hate speech, violence, gender or religious intolerance, child pornography, and drug or arms trafficking, that is, not with the causes, but with its consequences. This highlights the ineffectiveness of Ukraine's unauthorized information policy in combating disinformation disseminators in cyberspace.

Keywords: information policy, information environment, propaganda, disinformation, disinformation infiltration, strategic communication, manipulative content, information wars, cyberspace.

Introduction. In the context of modern geopolitical confrontations, the use of manipulative technologies as a means of information influence is a way to change the mass consciousness and social behavior of people. Manipulation of the collective consciousness (subconscious, unconscious) is a means of purposeful influence on the psyche of everyone to form the «necessary» public opinion and provoke certain events in society. The production of European values such as «freedom of speech» and «guarantee of self-expression» takes place against the backdrop of a total information glut, particularly fake information, in society and public consciousness in general, combined with the policy of «post-truth». It entails not only a hidden but also a real threat to modern society and the existence of democracy.

Methods. The research employed a combination of general scientific and specialized methods to ensure a comprehensive analysis of the phenomenon of disinformation and its impact on democratic institutions. In particular, the analytical method aims to identify the essence of manipulative technologies and the mechanisms by which they infiltrate the information space. In contrast, the comparative method seeks to contrast global and national approaches to countering disinformation, outlining differences in legal and communicative practices. Using the structural-functional method, the interaction among actors within the information environment is examined. The system approach provided a holistic understanding of disinformation as a multidimensional phenomenon combining technological, socio-psychological, and political-legal components. The prognostic method was applied to formulate conclusions and develop practical recommendations for enhancing mechanisms to counter disinformation infiltration.

Problem statement. In the practices of modern communication, public communication takes place through the transfer of information that affects the ideas and psyche of many. In addition, the era of virtual reality unfolds the possibilities of the human psyche at the subconscious level. At the same time, in the context of democratic transformations and against the backdrop of the formation of the virtual

world, public policy emerges as a form of communication aimed at revealing the hidden interaction between conscious activity and the unconscious of everyone, many, and all. Public policy is always related to ensuring the needs and interests of people in the context of exercising power and responsibilities in the activities of state institutions and civil society. Public communication, grounded in democratic principles and ideas, is a tool for building and enhancing various social institutions and shaping a new perspective on democracy in the digital realm.

Firstly, the information determines the further generation of knowledge and forecasting trends in the development of subject-object and subject-subject interactions, as well as social relations. In other words, a systematized and logically substantiated array of information about the needs, interests, feelings, moods, thoughts, motives, and behavior of people, including each individual and all individuals, serves as a fine-tuned tool for protecting the achievements of democracy. Consequently, a set of information about traditions, customs, symbols, and rituals forms the mentality of a national character and the fundamental values of a culture.

Results.

1. The impact of disinformation on society and democracy

Under this review, information communication unfolds as management and conscious influence on the part of the mediocracy, which can lead to a communicative crisis and, as a result, public distrust of existing media. In such circumstances, each individual and society as a whole are subjects and objects of the information space. The use of digital means of information exchange (disinformation) accessible to any person determines their self-identification in cyberspace as a socio-ecological and socio-media system of human and humane emergence in society, which in turn determines the universality of the process of mastering new knowledge through information and the practical self-realization of each and all. Such an order of things is absolutely possible in a democratic society since every individual has the right to freedom of thought and freedom of speech.

According to the popularity of user-generated content, the Internet can be divided into four main segments: «social knowledge», «social commerce», «social media», and «social networks». The latter two form social platforms that turn out to be not only a convenient tool for interpersonal communication, but also an environment for the penetration of various disinformation, including content of a threatening and immoral nature.

Therefore, there is a need for a meaningful expression of the concept of disinformation. First of all, it should be understood that «disinformation» is not only false information that has been deliberately and purposefully created/transformed/distorted to ensure coercion/harm/deception/ugliness towards an individual, social group, organization, or country [16], i.e., everyone-many-all. At the same time, the impact of disinformation, as a transformed and likely distorted form of communication, undermines the essence of interpersonal and social communication, serving as an instrument to erode democratic principles of delayed action. In this context, information warfare is primarily divided into «soft», which does not «work» directly with lies, and «hard», which replaces truth with lies with its further

promotion [10, с. 304]. Modern Ukraine is dealing precisely with the manifestation of a «brutal» information war in the information space.

Even in recent times, it can be argued that in countries with developed or growing economies that operate in the digital information space, there can be no total distortion of information. Given public access to the boundless space of world information, it was impossible to imagine that a «hard» information war could be likely. The prospect of forming one's own view of the state of affairs with the help of world sources of information is a manifestation of democracy and a manifestation of civilization, as well as an inseparable right of every person. However, thanks to many years of effort, mediocracy has led most members of society to form a habit of receiving ready-made answers, a coherent vision, and prepared thoughts, which have turned out to be the most convenient tool for influencing the consciousness of everyone. In particular, disinformation has become a weapon of «hard» information — primarily mental — war, and in a manipulative view, a necessary condition for the appropriate (unfortunately, distorted) formation of public opinion of different target audiences.

Therefore, it should be emphasized that an anti-constitutional content poses a particular danger to the state, which should include:

- 1) direct or indirect encroachment on national interests, territorial integrity, and democratic principles;
- 2) deliberate distortion of real socio-political processes and historical facts;
- 3) substitution of concepts and creation of mythologemes, as well as promotion of hostile narratives and values (traditions) of countries of external influence;
- 4) populism and manipulation in the application of political clichés to form a negative image of political «opinion leaders» and high-ranking officials.

At the same time, along with propaganda of hostility, terrorism, and drugs, especially dangerous in society is the purposeful dissemination of inappropriate — misleading, harmful, false, distorted, and manipulative — content directed against the individual (an element of cyberbullying), segregation of target audiences (taking into account language, age, religious, gender and social characteristics) and countries as a whole. After all, such content can provoke not only suicidal moods but also complete despondency of individuals and destabilization of society, as well as form a false, crazy idea among the population aimed at justifying murder.

The disinformation deployed in this area proves to be an effective tool for waging modern warfare, not only in the information space. The initial stage in the development of disinformation involves distorting content and producing pseudo-industrialized manipulations in cyber campaigns, which deliberately pollute the digital ecosystem of the global information space by influencing public opinion. At the next stage, disinformation unfolds from inciting ethnic hatred, anger, and rage towards representatives of other nationalities, to producing the idea of total extermination of some for the benefit of others, by justifying a war of conquest.

2. Disinformation infiltration: causes, mechanisms, and directions of counteraction

To combat fabricated social identities and the decontextualization of content, it is necessary to use various (including digital) tools to counteract infiltration, which

should minimize the pace and volume of disinformation spread in the cyber environment.

In a broad context, the phenomenon of disinformation infiltration should be understood not only as the usual penetration (ingress) of improper — hostile, false, harmful, ugly, misleading, fabricated, manipulative, superfluous — content into the information environment using digital technologies, but also its impact on the entire information, media and cyberspace of the country, and most importantly, on the mass consciousness of its citizens as consumers and users of such an information environment.

A high level of disinformation infiltration is observed not only during any manifestation of psychological impact and cyberbullying, including trolling, flaming, hating, grooming, and mobbing, but also during cybercrimes by phishing, carding, kidnapping, doxing, and ransomware (crypto extortion). In view of this, in previous studies [5], we have proposed some technological recommendations for combating the spread of dangerous content in the country's cyberspace, namely:

- 1) installation of blocking filters by Internet service providers without allowing users to turn them on or off;
- 2) application of algorithms for monitoring and filtering network traffic by artificial intelligence to detect or block access to illegal materials and tools for their distribution;
- 3) posting on the websites of an exceptional service to notify socially conscious users of information about the detection of harmful, illegal, and dangerous content;
- 4) forced blocking of websites that could potentially harm life, honor and dignity, business reputation, and health of citizens, as well as promote war, national and religious enmity, change of the constitutional order by violent means, or violation of the territorial integrity and independence of the country;
- 5) introduction of registration or activation of mobile SIM cards in the presence of an identity card (passport, ID card);
- 6) identification of users' digital devices (by IP address, MAC address, IMEI code);
- 7) control over points of public access to the Internet (Wi-Fi);
- 8) the obligation of ISPs to store metadata of users' Internet traffic and IP addresses (including dynamic IP addresses) provided to their digital devices for a specified period;
- 9) imposing obligations on the owners of Internet resources to store comments left by users (with the establishment of a specific period for storing such comments, including their storage on servers physically located in the country).

These recommendations have not lost their relevance so far, but at the same time require some rethinking, since democratic institutions, which guard modern society, are subject to devastating influence from information and disinformation attacks.

The tools, methods, and means proposed in previous studies [4] should not only be actualized and elevated to a higher level of information security, but also create an effective system for countering disinformation infiltration and ensuring the protection

of the interests of each individual, society, and state in the cyberspace of Ukraine. The country's cybersecurity system, as well as the institution for combating disinformation in the digital space, needs simultaneous and continuous improvement.

This can be achieved through the use of not only technological means but also the creation of an integrated complex of organizational, legal, socio-economic, and information-communicative (including ideological, value, and semantic) mechanisms of preventive, situational, and systemic nature. The main components of such a complex are:

Institutional and legal mechanisms:

- 1) normative definition of criteria for ranking and evaluating disinformation infiltration in the media and social media;
- 2) establishing requirements and rules for the functioning of mass media and media platforms in cyberspace (mandatory disclosure of information about their owners or founders, sources of funding, hosting, etc.);
- 3) application of strict restrictive measures by the state, represented by law enforcement agencies, to distributors of fabricated, harmful, dangerous, and manipulative content (removal and blocking in accordance with current legislation);
- 4) conducting informational and educational events among different groups of the population to convey information about the sources and types of disinformation;
- 5) Initiating the development and implementation of ethical codes in the digital space for government officials.
- 6) formation of the institution of responsibility for the dissemination of misinformation, for failure to fulfill the duties of officials to take measures to combat the dissemination of distorted information;
- 7) development and implementation at the international level of an instrument of interaction between states to prevent the spread of disinformation and bring to justice persons and states that disseminate false information.

Socio-economic mechanisms:

- 1) formation of an independent community of fact-checkers from civic activists and independent journalists to control and verify the accuracy of facts used in texts, speeches, «posts», etc.);
- 2) regulation and control over the distribution of advertising on hinged resources, in particular ensuring verification of the transparency and veracity of its sponsored political content (content), as well as limiting the possibility of targeting to minimize the income of disinformation providers in cyberspace;
- 3) ensuring appropriate conditions for the population to master digital competencies, the basics of media literacy, and cyber hygiene, in particular, encouraging and promoting the introduction of specialized educational media programs.

Information and communication mechanisms:

- 1) the use of value-sense means of information defense, in particular, conducting information and communication campaigns to disseminate positive narratives by «opinion leaders»;

2) formation of stable strategic communications of the state in the sphere of foreign and domestic policy to prevent the emergence of fakes and the distortion of information about real events in the state;

3) monitoring, moderating, and controlling measures to counteract the infiltration of fakes into cyberspace, in particular in online media and social media, based on legality, transparency, integrity, journalistic impartiality, and compliance with international human rights standards using their protection means;

4) stimulating the voluntary identification of all Internet users by means of modern digital technologies;

5) ensuring convenient, fast, and reliable access to all official documents, which is governed by the Council of Europe Convention on Similar Access to Official Documents.

3. Fighting disinformation: protection or threat to society?

Ukrainian legislation is outdated and lacks mechanisms to counter the spread of disinformation; its general norms also do not provide for liability for the transmission of false information. The lack of indicators and criteria for disinformation infiltration renders the normative definition and regulation of such content impossible, thereby avoiding responsibility for those who deliberately contribute to the dissemination of fake content in the media and on social media.

It should also be noted that sanctions mechanisms to counteract disinformation infiltration do not exist at the level of EU legislative acts. For example, only Lithuania is the only EU country where it is legally defined that disinformation is «deliberately publicly disclosed false information» (Zakon Lytovskoy Respublyky, 1996).

Disinformation fosters distrust of the government and democratic values among the population, posing a serious threat and causing significant harm to society. But in EU countries, spreading disinformation is not illegal. For example, apart from Germany, the regulation of social media and media is still not directly related to the prohibition of the dissemination of disinformation. Producers and disseminators of fake news are not criminally liable for their activities. Moreover, they are legitimately protected by the democratic right to freedom of speech and freedom of expression (freedom of expression). Therefore, in the EU countries, there is a struggle not against disinformation, but against cybercrime and the spread of illegal content related to extremism, racial hatred, hate speech, violence, gender or religious intolerance, child pornography, drug or arms trafficking, etc.

In 2015, to combat external disinformation in the European Union, the East StratCom (ESCTF) task force was established under the auspices of the European External Action Service, and on April 27, 2016, Regulation 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR) was adopted; Regulation (EU) 2016/679) on the protection of individuals about the processing of personal data and the free movement of such data within the European Union and the European Economic Area [11].

The Council of Europe adopted several documents on combating the spread of disinformation, namely: Parliamentary Assembly Resolution No. 2217 (2018) «Legal

challenges related to hybrid war and human rights obligations» [7], No. 2314 (2019) «Media Education in the new media environment» [8], No 2281 (2019) «Social networks: social flows or threats to human rights?» (Social media: social threads or threats to human rights?) [14], No 2255 (2019) «State media in the context of disinformation and propaganda» [9], No 2326 (2020) «Democracy broken? How to answer?» (Democracy hacked? It is noted that today states are increasingly dealing with manifestations of hybrid warfare, which has created a new type of threat, consisting of a combination of military and non-military methods, in particular, such as cyberattacks, massive disinformation campaigns, including fake news, distortion of facts and the use of manipulative technologies to convey lies to every member of society, primarily through social networks) [1].

The Parliamentary Assembly notes that digitalization, mobility, and online communication have provided undeniable benefits to the public, which has gained access to a wide range of information sources, including cultural, historical, political, economic, and technical content. The open nature of digital platforms contributes to the deployment of transparent and effective democracy. At the same time, in the digital age, threats to the realization of fundamental individual rights, democracy, and the rule of law are on the rise. A significant portion of the public, particularly young people, relies on social networks as their primary source of information. Disinformation and propaganda can affect not only elections and referendums, but also citizens' daily lives, political preferences, and trust in traditional media. To address disinformation, governments of Council of Europe member states should comply with Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries [12] and CM/Rec(2020)1 on the impact of algorithmic systems on human rights, as well as other relevant recommendation documents [13].

Thus, while the European Commission issues only recommendations on countering disinformation, and the EU Digital Services Act (DSA) was adopted in 2022, each EU country still independently chooses the specific measures to implement in practice [15].

In particular, on September 1, 2017, Germany adopted the Law «On Improving Law Enforcement in Social Networks» (hereinafter — NetzDG), which applies to Telemedia service providers who operate platforms on the Internet for profit. Such services are designed to enable users to share any content with other users or make it public (social networks)" [3].

Thus, social networks and media platforms with more than 40 million members (Facebook, YouTube, Reddit, Tumblr, and others) are usually subject to the provisions of this law. As a result, the number of user appeals to the police has increased significantly after several high-profile cases, when fake news and racist material spread through the German segment of well-known social networks were blocked. Social networks that fail to remove «illegal» posts could be fined up to €50 million. According to BBC NEWS, Facebook has hired several hundred new staff members in Germany to handle complaints about content that violates the NetzDG law, as well as to monitor and detect violations of content posted by regular users [2].

According to the NetzDG law, social networks must have an effective and transparent procedure for dealing with complaints about illegal content, provide users with a simple, easy-to-use, and permanently accessible procedure for filing complaints about unlawful content, which should ensure they immediately take note of complaints and check whether the content reported in the complaint is illegal. Additionally, it is determined that the content should be removed or blocked from access within 24 hours, and unlawful content should be removed within seven days of receiving the complaint. If removed, content is retained as evidence for ten weeks within the scope of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of the information society, in particular, electronic commerce in the internal market (Directive on electronic commerce, OJ L 178 of 17.7.2000, p. and Directive 2010/13/EC of the European Parliament and of the Council of 10 March 2010 on the coordination of specific laws, regulations and administrative provisions of the Member States relating to the provision of audiovisual media services (Audiovisual Media Services Directive, OJ L 95 of 15.4.2010, p. L 263 of 6.10.2010, p. 15), and which are governed by Directive (EU) 2018/1808 (OJ L 303, 28.11.2018, para. 69) [3].

In France, since October 15, 2021, under the interministerial body subordinate to the Prime Minister and the General Secretariat for Defense and National Security (Secr é tariat g é é ral de la D é fense et de la S é curit é nationale, SGDSN), Europe's first public service for combating manipulation of information in social networks — the Agency for Vigilance and Protection against External Digital Interference — was created [6]. The primary tasks of this service are to monitor, detect, and analyze the dissemination of hostile content by foreign states or non-governmental organizations through online digital platforms, and to promote or coordinate interagency work and international activities aimed at protecting France's fundamental interests against disinformation that may harm them.

Since November 1, 2022, a new state institution has been operating under the Swedish government to protect citizens from disinformation — the Psychological Protection Agency (<https://www.mpf.se>), which identifies, analyzes, and responds to misleading information that threatens the country's national interests. In particular, the said Agency provides appropriate countermeasures, for example, by developing methods and technologies to detect and respond to undue information influence. It also directs the work to coordinate the activities of authorities, the media, and other actors involved in psychological protection, thereby strengthening the media resilience of Swedish society and preventing the effects and consequences of disinformation infiltration.

At the same time, the primary tactic for combating the spread of disinformation in other EU countries is to enhance media literacy, foster critical thinking, raise public awareness of information attacks, and highlight the harmful impact of these on social processes. It is believed that the low level of digital competence and media literacy of Internet users is the reason for the increase in the level of illegal activities of hackers, cybercriminals, and cyber terrorists. However, civil society was not ready to increase its influence on the mass consciousness of information tools and digital technologies.

It also turned out that media literacy does not solve the problem of countering disinformation. Thus, by creating a danger of «fire in information flows, humanity did not take care of the institution of new information firefighters of the same level as the possible danger» [10, с. 3].

In Ukraine, any unauthorized information policy should be considered ineffective. After all, part of the state's territory is occupied, and the population is constantly the target of information attacks in the existing hybrid war. At the same time, the level of education and media literacy among the Ukrainian population varies, and the state must respond promptly and rigorously to today's challenges. It is also necessary to implement preventive measures to enhance the quality of general education and utilize specialized tools for media education, as well as the development of a critical attitude towards information among the population.

Conclusions. Thus, disinformation infiltration is an effective mechanism for influencing the collective consciousness of citizens immersed in the daily information and communication environment. The public tends to trust the information published in modern media. In view of this, the number of fakes and hidden propaganda is rapidly growing, which hurts the digital ecosystem of the global information space. Disinformation infiltration poses a global threat to democratic institutions and democracy itself, potentially becoming a significant factor in the ongoing crisis of democracy.

In our opinion, to improve the protection of democratic institutions not only in Ukraine but throughout the world, to form an effective system of cybersecurity and counter disinformation, it is necessary to introduce an integrated complex of socio-economic, organizational, legal, information, and communication mechanisms, namely:

- 1) formulate criteria for evaluating disinformation infiltration and dissemination of advertising on news resources;
- 2) establish requirements and rules for media activities in cyberspace;
- 3) determine restrictive measures by the state for disseminators of dangerous and manipulative content;
- 4) to provide conditions for the population to master digital competencies, the basics of media literacy, and cybersecurity;
- 5) introduce a system of monitoring and control of measures to counteract the infiltration of fakes into cyberspace in accordance with international standards.

To counter disinformation worldwide, it is necessary to establish an institution responsible for the dissemination of disinformation and harmful information, define indicators and criteria for identifying fake information, and provide mechanisms for regulation, control, and accountability for its dissemination.

The implementation of these criteria will reduce the prevalence of widespread disinformation and increase the overall level of information security and citizen education. At the same time, the primary measures for such implementation are not only ways to ensure the state's security but also tools for protecting democracy and democratic principles worldwide.

Producers and disseminators of disinformation on the Internet are virtual traitors to the state. Therefore, to effectively counteract covert disinformation campaigns against

the state (the primary goal, goals, objectives, and consequences of which are unknown), it is necessary first of all to deeply analyze the existing information environment (field) and possible target audiences for the spread of disinformation, to develop a strategy and tactics for the implementation of effective counteractions (counterpropaganda) by the authorities, to identify the perpetrators, resources and possible risks (threats), and to take into account the results of previous disinformation interventions against the state.

Література

1. Democracy hacked? How to respond? Parliamentary Assembly of the Council of Europe. Resolution 2326 (2020). URL: <https://pace.coe.int/en/files/28598/html> (дата звернення: 10.11.2025).
2. Germany starts enforcing hate speech law. BBC NEWS, 2018. URL: <https://www.bbc.com/news/technology-42510868> (дата звернення: 10.11.2025).
3. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz — NetzDG). Bundesamt für Justiz, 2021. URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (дата звернення: 10.11.2025).
4. Карпенко О. В. Вироблення стратегічних підходів та практичних рекомендацій із протидії поширенню в Україні дезінформації засобами соціальних медіа. *Вісник Національної академії державного управління при Президентові України*. Серія: Державне управління., 2021, № 1 (100), с. 7–14.
5. Карпенко О. В., Гавриляк В. Б. Ідентифікація користувачів мережі інтернет як механізм протидії поширенню небезпечного контенту в кіберпросторі України. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління., 2020, вип. 1 (12), с. 211–227.
6. Le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM). 2021. URL: <http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etranangeres-viginum> (дата звернення: 10.11.2025).
7. Legal challenges related to hybrid war and human rights obligations. Parliamentary Assembly of the Council of Europe. Resolution 2217 (2018). URL: <https://pace.coe.int/en/files/24762> (дата звернення: 10.11.2025).
8. Media education in the new media environment. Parliamentary Assembly of the Council of Europe. Resolution 2314 (2019). URL: <https://pace.coe.int/en/files/28302> (дата звернення: 10.11.2025).
9. Public service media in the context of disinformation and propaganda. Parliamentary Assembly of the Council of Europe. Resolution 2255 (2019). URL: <https://pace.coe.int/en/files/25406> (дата звернення: 10.11.2025).
10. Почепцов Г. Г. Пропаганда 2.0. Харків: Фоліо, 2018. 791 с.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016... (General Data Protection Regulation). *Official Journal of the European Union*. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 10.11.2025).
12. Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. 2018. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e14 (дата звернення: 10.11.2025).

13. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. 2020. URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 (дата звернення: 10.11.2025).

14. Social media: social threads or threats to human rights? Parliamentary Assembly of the Council of Europe. Resolution 2281 (2019). URL: <https://pace.coe.int/en/files/27681> (дата звернення: 10.11.2025).

15. The Digital Services Act: ensuring a safe and accountable online environment. 2021. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (дата звернення: 10.11.2025).

16. Wardle C., Derakshan H. Information disorder: toward an interdisciplinary framework for research and policymaking. Strasbourg: Council of Europe, 2017.

References

1. Democracy hacked? How to respond? Parliamentary Assembly of the Council of Europe. Resolution 2326. 2020. Accessed November 10, 2025. <https://pace.coe.int/en/files/28598/html>.

2. Germany starts enforcing hate speech law. *BBC News*. 2018. Accessed November 10, 2025. <https://www.bbc.com/news/technology-42510868>.

3. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG). Bundesamt für Justiz. 2021. <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (Accessed November 5, 2025).

4. Karpenko, O. V. «Vyroblennia stratehichnykh pidkhodiv ta praktychnykh rekomendatsii iz protydii poshyrenniu v Ukraini dezinformatsii zasobamy sotsialnykh media» [Developing Strategic Approaches and Practical Measures to Counter the Spread of Disinformation in Ukraine through Social Media]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Seriya: Derzhavne upravlinnia* 1 (100). 2021: 7–14. [in Ukrainian].

5. Karpenko, O. V., and V. B. Havryliak. «Identyfikatsiia korystuvachiv merezhi internet yak mekhanizm protydii poshyrenniu nebezpechnoho kontentu v kiberprostorii Ukrainy» [Identifying Internet Users as a Mechanism for Counteracting the Spread of Dangerous Content in Ukraine's Cyberspace]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy* 1 (12). 2020: 211–227. [in Ukrainian].

6. Le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM). 2021. <http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangees-viginum> (Accessed November 5, 2025).

7. Legal challenges related to hybrid war and human rights obligations. Parliamentary Assembly of the Council of Europe. Resolution 2217. 2018. <https://pace.coe.int/en/files/24762> (Accessed November 5, 2025).

8. Media education in the new media environment. Parliamentary Assembly of the Council of Europe. Resolution 2314. 2019. <https://pace.coe.int/en/files/28302> (Accessed November 5, 2025).

9. Public service media in the context of disinformation and propaganda. Parliamentary Assembly of the Council of Europe. Resolution 2255. 2019. <https://pace.coe.int/en/files/25406> (Accessed November 5, 2025).

10. Pocheptsov, H. *Propahanda 2.0* [Propaganda 2.0]. Kharkiv: Folio, 2018. [in Ukrainian].

11. Regulation (EU) 2016/679... (General Data Protection Regulation). *Official Journal of the European Union*. 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (Accessed November 5, 2025).

12. Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries. 2018. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e14 (Accessed November 5, 2025).

13. Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems. 2020. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 (Accessed November 5, 2025).

14. Social media: social threads or threats to human rights? Parliamentary Assembly of the Council of Europe. Resolution 2281. 2019. <https://pace.coe.int/en/files/27681> (Accessed November 5, 2025).

15. The Digital Services Act: Ensuring a Safe and Accountable Online Environment. 2021. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (Accessed November 5, 2025).

16. Wardle, Claire, and Hossein Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Strasbourg: Council of Europe, 2017.

ДЕЗІНФОРМАЦІЙНА ІНФІЛЬТРАЦІЯ: ФЕНОМЕН ВИНИКНЕННЯ ТА МЕХАНІЗМИ ПРОТИДІЇ

Карпенко Олександр Валентинович

доктор наук з державного управління,
професор,
завідувач кафедри національної економіки та
публічного управління,
Київський національний економічний
університет
імені Вадима Гетьмана, Україна

ORCID: <https://orcid.org/0000-0002-9301-7973>

Цимбаленко Яна Юріївна

кандидат наук з державного управління,
доцент,

докторант кафедри національної економіки
та публічного управління,
Київський національний економічний
університет

імені Вадима Гетьмана, Україна

ORCID: <https://orcid.org/0000-0003-0442-7549>

Савченко Наталія Володимирівна

доктор наук з державного управління, с.н.с.,
Національне агентство України

з питань державної служби, Україна

ORCID: <https://orcid.org/0000-0002-4585-1787>

Анотація. У статті обґрунтовано виникнення соціально-філософського феномену дезінформаційної інфільтрації та проаналізовано наслідки її впливу на суспільство. Надано авторське визначення поняття «дезінформаційна інфільтрація» та запропоновано механізми протидії проникненню незаконного, небезпечного, шкідливого, хибного, оманливого та маніпулятивного контенту в кіберпростір України. Виявлено недосконалість українського законодавства, яке не регламентує інструменти протидії дезінформації, а також не передбачає відповідальності за поширення неправдивої інформації. Обґрунтовано, що дезінформація породжує суспільну недовіру до органів державної влади та демократичних цінностей, що становить серйозну загрозу та завдає значної шкоди суспільству. Ідея про те, що дезінформаційна інфільтрація є однією з причин кризи демократії, чітко постає як гіпотеза для подальших наукових досліджень. Наголошується, що відповідно до європейських стандартів дезінформація не вважається незаконною, і її поширення законом не забороняється. Крім того, виробники фейкових новин прямо чи опосередковано захищені демократичним правом на свободу слова та свободу вираження поглядів. Країни ЄС борються не з дезінформацією, а з кіберзлочинністю та поширенням незаконного контенту, пов'язаного з екстремізмом, расовою ненавистю, мовою ворожнечі, насильством, гендерною або релігійною нетерпимістю, дитячою порнографією, торгівлею наркотиками або зброєю — тобто не з причинами, а з наслідками. Це визначає неефективність застосування в Україні несанкційної державної (інформаційної) політики проти поширювачів дезінформації в кіберпросторі.

Ключові слова: інформаційна політика, інформаційне середовище, пропаганда, дезінформація, дезінформаційна інфільтрація, стратегічна комунікація, маніпулятивний контент, інформаційні війни, кіберпростір.

Стаття надійшла до редакції 08.11.2025

УДК 336.27

JEL Classification: H63, E62, G15, O23

DOI: <https://doi.org/10.33111/sedu.2025.57.103.117>

Онишко Світлана Василівна*

Вергелюк Юлія Юріївна**

Ганцяк Михайло Олегович***

СУЧАСНІ МЕТОДИ ТА ІНСТРУМЕНТИ ВИРІШЕННЯ БОРГОВИХ ПРОБЛЕМ УКРАЇНИ

Анотація. У статті акцентується увага на необхідності пошуку ефективних рішень для подолання боргових проблем України. Зокрема, акцент

* **Онишко Світлана Василівна** — доктор економічних наук, професор, професор кафедри фінансових ринків та технологій, Державний податковий університет (Ірпінь, Україна), ORCID: <https://orcid.org/0000-0001-9073-6166>, e-mail: onyshko_sv@ukr.net

** **Вергелюк Юлія Юріївна** — кандидат економічних наук, доцент, доцент кафедри фінансових ринків та технологій, Державний податковий університет (Ірпінь, Україна), ORCID: <https://orcid.org/0000-0003-1773-6631>, e-mail: strchk81@gmail.com

*** **Ганцяк Михайло Олегович** — доктор філософії (PhD), начальник відділу фінансової політики, Державний науково-дослідний інститут інформатизації та моделювання економіки, (Київ, Україна), ORCID: <https://orcid.org/0000-0002-6136-3193>, e-mail: m.hantsyak@ukr.net