

DISINFORMATION IN THE MEDIA: NEW CHALLENGES FOR LAW ENFORCEMENT AGENCIES OF UKRAINE AND COUNTERMEASURE TECHNOLOGIES UNDER MARTIAL LAW

Nehrebetskyi V. V.

INTRODUCTION

In the context of modern hybrid warfare, information becomes not just a communication tool, but a real weapon that can influence mass consciousness, destabilize society and undermine confidence in state institutions. Disinformation as a key element of this information confrontation is widely used by hostile forces to manipulate public opinion, create panic and spread fakes.

This problem is particularly acute in Ukraine, where the war is being waged not only on the battlefield, but also in the media space. Enemies of the state actively use propaganda, fake news and distorted information to weaken the morale of citizens and international support. In such circumstances, the search for effective methods to combat disinformation becomes a strategically important task.

The aim of the study is to analyze the problem of disinformation in the field of mass media in the context of the war in Ukraine, identify the main mechanisms of its spread and evaluate modern technologies used to counter information attacks. The study also examines government initiatives, international experience, and promising strategies for protecting the information space aimed at minimizing the impact of disinformation and strengthening the media sustainability of society¹.

Ensuring information security of Ukraine is one of the most important functions of the state. Presidential Decree No. 685/2021 of December 28, 2021 approved the decision of the national security and Defense Council of Ukraine of October 15, 2021 "On the Information Security Strategy of Ukraine"². The Information Security Strategy defines current challenges and threats to the national security of Ukraine in the information sphere,

¹ Note. The article was written within the framework of the development of the fundamental topic "Prioritization and technologization in criminal proceedings in wartime and post-war times", which is being studied by specialists of the Research Institute for the Study of Crime Problems named after Academician V. V. Stashys of the National Academy of Sciences of Ukraine.

² Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.21 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>

strategic goals and objectives aimed at countering such threats, protecting the rights of individuals to information and protecting personal data. The implementation of the strategy is designed for the period up to 2025.

The goal of the strategy is to strengthen the ability to ensure information security of the state, its information space, support social and political stability, State defense, protection of state sovereignty, territorial integrity of Ukraine, democratic constitutional order, ensuring the rights and freedoms of every citizen by information means and measures.

The 21st century is characterized by the rapid development of innovative digital technologies, the purpose of which is to increase the efficiency of human activity, improve comfort and work results. The development of the information space in the context of globalization and the COVID-19 pandemic have led to the strengthening of the role of social networks in the national and global information space, their impact on the internal and external socio-political situation, the state of respect for Human Rights and freedoms, in particular, to ensure the principles of equal rights of users of social networks.

At least the right to privacy (protection of confidential information about a person, non-interference in privacy) is one of the fundamental human rights, which is enshrined in the Universal Declaration of human rights, the convention for the protection of human rights and fundamental freedoms, other international documents, as well as the constitutions of most states of the world, digital transformations are also changing this sphere. The increase in the number of social networks, their integration with other social services of everyday use, as well as the specifics of the organization of the World Wide Web jeopardize the guarantees of a person's right to privacy. Attempts to resolve this problem continue, and new approaches are being formed to ensure the balance of the right to privacy and information security of the state.

A significant expansion of sources of access to information in the context of the rapid development of digital technologies and at the same time insufficient level of media literacy (media culture) is accompanied by a decrease in the criticality of information perception, creates the basis for possible manipulation of public opinion, which contributes to the growth of the influence of disinformation and destructive propaganda, the popularity of conspiracy theories. Uncritical perception of information poses threats to the political and economic stability of Democratic states.

The work of many Ukrainian information security specialists, such as O.O. Vergolyas, D.V. Vedenev, O.G. Zaruba, Yu.I. Kogut, O.R. Lebedev, O.V. Litvinenko, V.A. Lipkan, N.V. Netesa, V. Moklyak, V.Ya. Novitsky, V.M. Panchenko, O.P. Dzeban, V.G. Pilipchuk, V.M. Furashev, D.V. Lande and others, was devoted to the

issues of legal security in the information space and countering Special information operations in the context of the security and defense sector of Ukraine³.

In recent years, the attitude to information security in Ukraine has undergone significant changes. First of all, the very nature of this phenomenon was transformed, and with it the strategic dimension of the concept of ensuring national Information Security. Today, it is no longer perceived as something abstract or exclusively theoretical. On the contrary, this is a real and extremely acute area of confrontation, in which fierce battles unfold, and threats have very specific and tangible consequences.

In the context of a large-scale information war against Ukraine, one of the key challenges is the legal support of the strategic concept of Information Security. Pre-war developments in this area have become an important basis for further development and scientific research. However, modern realities require not only rethinking existing approaches to the legal regulation of the information sphere, but also realizing that the legal component of national security depends on the security of the information space. At the same time, certain aspects of legal support for information security under martial law remain insufficiently studied. This requires a more detailed analysis of this issue, which will allow both to deepen the scientific understanding of the issue, but also to develop effective mechanisms for countering modern threats.

It should be noted that in the literature sources and at scientific events, certain aspects of the use of modern innovative digital technologies in the context of ensuring information security were mainly considered. At the same time, not all existing technologies were the subject of research, so the issue of using information technologies, in particular modern technologies for detecting and countering fakes, requires further research. The problem of using digital evidence also remains relevant, since unlike traditional "non-digital" evidence, all these documents are generated digitally and stored on digital platforms. In connection with the war in Ukraine, the issue of developing and implementing a long-term strategy for protecting the information space of Ukraine is extremely relevant. This is explained by the fact that the war against Ukraine from the very beginning had a "hybrid" character, that is, information attacks and sabotage in communication networks were simultaneously used, so the study of the issue of countering Special information operations is very relevant.

³ Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право*. 2023. № 3(46). С. 98–107. URL: <http://il.ippi.org.ua/article/view/287168>

1. Disinformation in the media as a tool of hybrid warfare

The beginning of military aggression against Ukraine in 2022 was closely linked to the strong information influence of the enemy on our society through hybrid warfare technologies. This was made possible by the active use of information technologies, and the influence of innovative tools for the exchange and transmission of information in various information resources.

Unfortunately, not all information search technologies are equally equivalent, safe, and resistant to illegal information influence. In 2023, Google introduced Search Generative Experience (SGE) technology⁴. This search service is carefully designed and trained to identify and present to the user high-quality results that match and support the information in the search results. By combining state-of-the-art combinations of language models and targeted teaching methods, Google has created a search engine that provides reliable and verified information. Google aims to prevent malicious, offensive, or explicit content from being displayed in its ranking systems. The search Generative Experience (SGE) technology that search is based on is designed for this purpose. The main focus is on creating informative responses, confirmed by reliable sources, so that users receive truthful and verified information. In cases where Google systems have less trust in the source or face information gaps, the goal is to avoid providing images generated by artificial intelligence. In addition, explicit or dangerous topics are deliberately avoided to maintain a responsible and secure search environment.

Of course, personalized information selection technologies have a great future and provide many advantages to people who are studying or improving their professional level. But unfortunately, any tool in the hands of the offender can turn into evil. And if we are talking about information technology, then the strength of this disaster increases many times. So, messengers, as well as social networks, which almost everyone has access to, provide the most opportunities for distributing almost any information. It is possible not just to spread the news once, but to start a "chain reaction", when the news is repeatedly forwarded by users of the social network from one person to a whole group of people, or even to other social networks.

It is a pity that not all information resources are able to identify unreliable sources of information. News and messages may not correspond to reality⁵. Fake means an object that is made to look real or valuable in

⁴ Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: <https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html>

⁵ Аналітичний звіт «російський інформаційний вплив в Африці». URL: <https://cpd.gov.ua/reports/analychnyj-zvit-rosijskyj-informacijnyj-vplyv-v-afryci/>

order to deceive people⁶. Thus, fake information is deliberately false. Disinformation-information designed to mislead a person⁷.

There are three types of information that can characterize fakes:

- Disinformation – false and deliberately created to cause harm to a person, social group, organization or country information;
- False information – misinformation) – false, but created without the intention of causing harm, information;
- Malinformation – information based on real facts is used to cause harm to a person, organization or country⁸.

Of particular importance is the issue of responsibility for the dissemination of information that threatens the national security of Ukraine, namely, aimed at harming the sovereignty, territorial integrity and inviolability, defense capability, state, economic or information security of the state. Thus, the enemy is trying to methodically and consistently undermine the authority of the state and authorities, and weaken the country's defense capability. On April 19, 2023, draft law No. 9223 "On amendments to the criminal and criminal procedure codes of Ukraine concerning the establishment of responsibility for certain actions against the foundations of national security of Ukraine" was submitted to the Verkhovna Rada of Ukraine⁹. The explanatory note to the draft law states that "Russian special services are increasing their efforts to use a new tool of information warfare in the interests of the aggressor country. Instagram Facebook, Instagram and Twitter networks of accounts (accounts) that contain false data about users. These are so-called botnets, whose activities are coordinated from the outside and united by a single goal, in particular, such as holding actions of information influence against the state interests of Ukraine. Citizens of Ukraine are also issued for such actions.

Thus, the Security Service of Ukraine identified and stopped functioning in 2022 – 45 bot farms with a total capacity of more than 4 million bots whose activities were distributed to multi-million audience users of social networks in different regions of Ukraine (and not only). At the same time,

⁶ Fake. URL: <https://dictionary.cambridge.org/dictionary/english/fake>

⁷ Велика українська юридична енциклопедія: У 20 т. Т.20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків: Право, 2018. 952 с.

⁸ Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008). URL: <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>

⁹ Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України / ВР України. URL: itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxhEwLZ_ZpX_M61T0/

the measures taken exposed and blocked about 11 thousand accounts that were used in favor of the Russian occupiers. It is also not uncommon for users of accounts to pretend to be other persons, in particular representatives of the authorities, other public persons to whom special attention is focused, and on behalf of these persons post and distribute various false, manipulative information in social networks and on other internet platforms. In addition, with the growing influence of social networks, the problem of "information bubbles" has become more acute, when people are surrounded only by information that confirms their own views and beliefs. This phenomenon can create the illusion of the same thinking in a group of people and lead to isolation from other views, a decrease in diversity of opinions, and even an aggravation of conflicts. At the same time, people tend to create "information bubbles" around them: they block content in social networks or do not perceive content that does not correspond to their preferences. They also respond more actively and spread what suits their interests and emotions. Social media algorithms adapt to such user desires and eventually stop offering alternative views in the feed altogether. So, after viewing certain content several times, the social network's algorithms will be more active in offering just such information in the future¹⁰.

Unfortunately, social networks do not respond very much to messages about fake profiles and pages that are involved in information attacks. Therefore, there is a need to increase control by law enforcement officers. What information is freely available, it is possible to use the method of collecting and analyzing information from open sources (*Open source intelligence, OSINT*).

Countering such sophisticated misinformation requires not only technological solutions, but also a comprehensive approach. Increasing media literacy is critical to enabling the public to identify and understand the tactics used in disinformation campaigns. Social media platforms should also take responsibility by improving the detection and removal of fake accounts and working with fact checkers to ensure transparent content moderation. In addition, the regulatory environment must evolve to hold social media platforms accountable for the content they distribute and protect user data from exploitation. Governments and international organizations should consider regulations that address these issues,

¹⁰ Як не стати жертвою шахраїв та ворожої пропаганди: кіберполіція про фактчекінг (02 травня 2024 р.). URL: <https://cyberpolice.gov.ua/article/yak-ne-staty-zhertvoyu-shaxrayiv-ta-vorozhoyi-propagandy-kiberpolicziya-pro-faktcheking-437/>

balancing the need for freedom of expression and the imperative of preserving the integrity of information¹¹.

Finally, it is necessary to emphasize the importance of vigilance, technological literacy and compliance with ethical standards in the complex interaction of narratives and artificial intelligence in social networks. For journalists, content creators, and social media users, understanding this dynamic is key to effectively countering disinformation and defending the truth in our increasingly interconnected world.

Social media platforms such as Facebook and X (formerly Twitter) have become key players in the artificial intelligence-driven disinformation landscape. The emergence of generative AI has significantly increased the spread and sophistication of disinformation campaigns. These campaigns are increasingly using artificial intelligence tools to create and disseminate misleading information on an unprecedented scale. These media platforms also face the problem of moderation of content created by artificial intelligence.

2. Modern technologies for detecting and countering disinformation

In today's information space, where disinformation poses a serious threat to democratic processes, the role of fact-checking is becoming more important than ever. Today, there is a growing interest in studying the mechanisms of detecting falsifications in the media, both from the academic community and among practicing journalists. Ukrainian media experts, based on the best international experience in the field of fact-checking and information verification, are actively adapting and improving their own methods for recognizing false statements.

Fact-checking is the process of verifying information for accuracy. Fact-checking has become an integral part of modern journalism and everyday life. In an era when information travels at the speed of light, the importance of fact-checking cannot be overemphasized. According to a study by the American organization "Duke Reporters' Lab", today there are 446 fact-checking organizations in different countries of the world¹².

The fact checker verifies information exclusively on the basis of open and official sources. The key difference between factoring and investigative journalism is the fundamental rejection of the use of insider, anonymous or unofficial information as an evidence base. In the process of verification, fact checkers rely on official data from Ukrainian and foreign government

¹¹ Посібник для творців контенту для виявлення та протидії російській пропаганді в нових технологіях. (За підтримки Уряду Великої Британії в рамках проекту «Розуміння штучного інтелекту»). 2024. URL: https://ai.instingov.org/assets/guide/AI-Guide_uk.pdf

¹² Fact-Checking. URL: <https://reporterslab.org/fact-checking/>

bodies, international organizations, scientific institutes, as well as official responses to requests sent to relevant institutions.

To verify information, fact checkers use data from official sources, such as:

State statistics service of Ukraine,
Ministry of Finance of Ukraine,
State treasury service of Ukraine,
The Verkhovna Rada Of Ukraine,
Cabinet Of Ministers Of Ukraine,
National Bank of Ukraine,
International Monetary Fund,
The World Bank and other reputable organizations.

Additional recommendations for verifying information are provided in the "Verification Handbook" published by the European Center for journalism¹³. In this manual, internationally recognized editors and journalists share methods for checking content for accuracy. It contains a list of online tools that allow you to verify: text publications, photo and video materials, primary sources of information, the identity of information distributors, and social media accounts.

Fact-checking is a type of journalistic investigation and includes basic structural elements similar to traditional journalistic analysis. These include:

1. Object of research – a verifiable statement, fact, or information.
2. Evidence base – official data, documents, and confirmed sources.
3. References to competent sources-state bodies, scientific institutes, international organizations and other reputable resources.
4. Expert comments – expert opinions that contribute to an objective assessment of information.
5. Logical conclusion, final conclusion about the reliability of the fact being checked¹⁴.

Fact-checking consists of several key semantic blocks:

1. *The object of verification* is a public statement (less often-a resonant fact) that is being investigated.
2. *The essence of the issue* is an informational preamble containing explanatory materials preceding the evidence base.
3. *Evidence and arguments* – confirmed facts, statistics, documents and certificates obtained exclusively from open official sources, as well as expert opinions supported by links to authoritative resources.

¹³ Посібник з верифікації. Центр Європейської Журналістики; Асоціація Видавців (УАВПП). 2014. URL: https://verificationhandbook.com/book_ua

¹⁴ Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи. Практичний посібник. Дніпро : ЛІРА, 2017. 133 с.

4. *Verdict* – a final conclusion on the reliability of information with a brief reasoned explanation.

The verdict in fact-checking has a clear structured form and is based on objective criteria, which avoids subjectivity and value judgments. In Ukrainian practice, three types of verdicts are used:

1. "Pravda" – information corresponds to facts.

2. "Half-truths" – information contains both reliable and distorted or manipulative elements.

3. "Untrue" – the information is completely unreliable.

The basic information verification protocol for fact checkers includes several consecutive stages:

1. Material detection – identification of statements that require verification.

2. Selecting the verification method – determining the fastest and most efficient verification method.

3. Information search – analysis of data from recognized authoritative sources to confirm or refute a fact, classify it as true, false, manipulative or questionable.

4. Analysis and justification – the study of a selected fact with a reasoned justification of the chosen verification method and presentation of the results.

5. Expert review – assessment of the reliability of sources and the correctness of their classification.

6. Cross – fact checking-the final verification of the logical sequence of information. In case of inconsistencies, the material is corrected taking into account expert comments.

7. Involvement of external experts (if necessary) – for additional evaluation of the text.

8. Publication of verified information – submission of final data with mandatory links to sources and indicating the contribution of experts to the verification process¹⁵.

Among the fact-checking platforms of Ukrainian developers, it is necessary to mention the mantis Analytics platform (2023)¹⁶. The last uses artificial intelligence to detect fake information and misinformation in online media and social networks. Mantis processes thousands of messages and gigabytes of data in real time, and then presents the data on an interactive map.

¹⁵ Ейсмунт В. Інструменти фактчекінгу: як професійно відрізнити брехню від правди. Інститут масової інформації. URL: <https://imi.org.ua/articles/instrumenti-faktchekingu-yak-profesiyno-vidriznyati-brehyu-vid-pravdy-i407>

¹⁶ Mantis Analytics. URL: <https://mantisanalytics.com/>

In 2022, the fact check bot "Perevirka" was launched in the Telegram messenger¹⁷. The Center for countering disinformation under the national security and Defense Council of Ukraine recommends this bot-a savior from fake news, unverified information¹⁸. To check the information, just send the news to the bot. The team of the fact check Department of Guara Media processes information sent by users of the bot "Perevirka" and facts that are viral or socially dangerous. Fact checkers can assign 5 statuses to requests sent to the verification bot, as well as send it for a more in-depth check. Possible statuses: True; Fake; Half-truth; No evidence; Refusal.

"True" means that information reflects the real situation in life without distorting any aspect of it. Truthful information – factually reliable, presented in the right context.

The status "True" implies that reliable sources confirm the information. However, it is assumed that the fact checker has chosen more than one source to confirm the fact, except in cases where the source is the only one covering this topic.

"Fake" means that this information is completely unreliable, fictitious, deceptive – there were no corresponding events, situations, or phenomena at all. False information is one whose fake nature can be proved.

"Half-truth" (manipulation) – a statement that contains elements of truth and untruth in certain proportions. Semi-true information misleads the audience by presenting information in a distorted context. Requests that acquire the status of "half-truths" require a comment – a brief analysis of the main conflicts between true and false data.

"Lack of evidence" – information that cannot be supported by evidence in any way. Information from such requests does not have reliable confirmation in the public domain.

"Refusal" is a status that receives a request that cannot be verified for technical or other reasons. So you should leave a refusal if:

1. does not contain any problematic facts (the request contains only the brand name, a call for a photo without accompanying text);
2. unavailable (outdated or blocked call);
3. the request is unconstructive (nonsense, unethical, entertainment);
4. information cannot be verified in real time (data on the take-off of bombers, or the sounds of explosions in the region).

Additional function – "Escalation". Escalation is an additional function that is necessary to determine the need for more detailed verification of a given request. When using this feature, the user will be notified that

¹⁷ Фактчек-бот "Перевірка". URL: https://t.me/perevir_bot

¹⁸ Центр протидії дезінформації при РНБО рекомендує новий фактчек-бот "Перевірка" (18.03.2022). URL: <https://imi.org.ua/news/tsentr-protidyiyi-dezinformatsiyi-pry-rnbo-rekomenduye-novyy-faktchek-bot-perevirka-i44450>

their request requires more time to analyze. After processing the request, it should be assigned one of the above statuses: true, fake, half-truth, or lack of evidence.

After assigning the status, the fact checker provides a comment if necessary. Response comment-a concise text that justifies and explains the status assigned to the request. By submitting a comment to a request, the fact checker generates it in compliance with the fact-checking policy that follows the fact-checking Department of Gwara Media. The commentary contains explanations and references to the sources on the basis of which conclusions are drawn. The comment received by the user allows them to independently check the correctness of the information provided by the fact checker by reproducing the search path for this information.

The speed of Request Verification occurs according to the following distribution:

"Quick requests" – are processed no longer than 24 hours, since the response to this request is publicly available and does not require detailed technical verification;

"Slow requests" – are determined by assigning an escalation status and are processed within 7 days, since there is a need for in-depth analysis of information.

The fact checker can contact the user to clarify the request. To do this, the bot has a "Dialog with initiator" function. It initiates a message to the user on behalf of the fact checker via the bot. however, it is worth noting that the initiator's personality is not tracked, since communication takes place through the Dialog in the bot.

According to the fact-checking policy on the website of the fact-checking department for refuting fake news that has signs of a virtual or dangerous component. The published material may have the status "Fake" or "Half-Truth" (manipulation). Verification is similar to the methodology for checking notebooks with bots¹⁹.

3. Prospects and strategies of Information Protection in Ukraine

Regulatory and legal regulation of information security, including in the Internet Information Network, is carried out by the Constitution of Ukraine, laws of Ukraine, presidential decrees and resolutions of the Cabinet of ministers and the Verkhovna Rada. The basis of Information legislation is, in particular, the laws: "On information", "On information protection in information and telecommunications systems", "On personal data protection", "On electronic documents and electronic document

¹⁹ Методологія фактчекінгу Гіара Медіа. URL: <https://gwaramedia.com/metodologiya-faktchekingu-perevirka/>

management", "On electronic trust services", "On the National Police", "On the National Geospatial Data Infrastructure", "On access to public information", "On the basic principles of ensuring cybersecurity of Ukraine".

Bylaws in the field of information security play a key role in the system of legal regulation, ensuring the practical implementation of strategic decisions. They establish specific rules, procedures and standards that detail and complement the core principles laid down in government strategies and programs. Thanks to these acts, the activities of state bodies, enterprises and other entities become more systematic and orderly, which contributes to the effective implementation of information security policies. This approach allows not only to increase the level of security of information resources, but also to minimize the risks of threats, which is critical for national security and state sustainability.

In particular, the following regulatory legal acts play this role, including the Decision of the National Security and Defense Council of Ukraine of April 28, 2014 "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine"²⁰, National Security Strategy of Ukraine, approved by Decree of the President of Ukraine dated 14.09.20 No. 392/2020²¹, Military Security Strategy of Ukraine, approved by Decree of the President of Ukraine dated 03/21/21 No. 121/2021²², Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine dated 08/26/21 No. 447/2021²³, Information Security Strategy, approved by Decree of the President of Ukraine dated 12/28/21 No. 685/2021²⁴, Strategy for ensuring state security, approved by Decree of the President of Ukraine dated

²⁰ Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ в.о. Президента України від 01 травня 2014 р. № 449/2014 URL: <https://zakon.rada.gov.ua/laws/show/449/2014#Text>

²¹ Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>

²² Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 21.03.21 р. № 121/2021. URL: <https://www.president.gov.ua/documents/1212021-37661>

²³ Про рішення Ради безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

²⁴ Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.21 р. № 685/2021.

URL: <https://www.president.gov.ua/documents/6852021-41069>

16.02.22 No. 56/2022²⁵, as well as plans adopted for their implementation: Implementation Plan of the Cybersecurity Strategy of Ukraine, put into effect by Decree of the President of Ukraine dated 01.02.22 No. 37/2022²⁶, Action Plan for the Implementation of the Information Security Strategy for the Period Until 2025, Approved by Order of the Cabinet of Ministers of Ukraine No. 272-r of March 30, 2023²⁷, Action Plan for the Implementation of the Strategy for Ensuring State Security, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 18.04.23 No. 318-r²⁸, as well as departmental regulatory legal acts of law enforcement agencies of Ukraine.

The Information Security Strategy (approved by Decree of the President of Ukraine dated 28.12.21 No. 685/2021) identifies current challenges and threats to the national security of Ukraine in the information sphere, among which, in relation to the influence of modern mass media, the following were highlighted:

- Social networks as subjects of influence in the information space;
- Insufficient level of media literacy (media culture) in the conditions of rapid development of digital technologies;
- Limited opportunities to respond to disinformation campaigns;
- Immaturity of the strategic communications system;
- Insufficient level of information culture and media literacy in society to counteract manipulative and informational influences²⁹.

In order to implement the tasks set, the Information Security Strategy of Ukraine introduces basic concepts, among which we will separately highlight the following:

Information security of Ukraine – is a component of the national security of Ukraine, a state of protection of state sovereignty, territorial integrity, democratic constitutional order, other vital interests of man, society and the state, under which constitutional rights and freedoms of man to collect, store, use and disseminate information, access to reliable and objective information are properly ensured, there is an effective system

²⁵ Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року “Про Стратегію забезпечення державної безпеки”: Указ Президента України від 16.02.22 р. № 56/2022. URL: <https://www.president.gov.ua/documents/562022-41377>

²⁶ План реалізації Стратегії кібербезпеки України: Указ Президента України від 01.02.22 р. № 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>

²⁷ Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text>

²⁸ Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України від 18.04.23 р. № 328-р. URL: <https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text>

²⁹ Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”: Указ Президента України від 28.12.21 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>

of protection and counteraction to harm caused by the spread of negative information influences, including the coordinated spread of unreliable information, destructive propaganda, other information operations, unauthorized distribution, use and violation of the integrity of information with limited access.

Information threat – potentially or actually negative phenomena, trends and factors of information impact on a person, society and the state, which are used in the information sphere in order to make it impossible or difficult to implement national interests and preserve national values of Ukraine and may directly or indirectly harm the interests of the state, its national security and defense;

Information measures of state defense – a set of coordinated actions that are prepared and carried out by entities ensuring national security and defense of Ukraine in peacetime, in a special period, in conditions of war or a state of emergency regarding the prediction and detection of information threats in the military sphere, prevention, deterrence and repulsion of armed aggression against Ukraine, counteraction to information threats from the aggressor state, as well as the implementation of other necessary actions in the information confrontation;

Strategic narrative – a specially prepared text intended for verbal presentation in the process of strategic communications for the purpose of information impact on the target audience.

There are four groups of actors involved in countering disinformation in Ukraine:

- public authorities (including representatives of the political arena);
- individual citizens;
- representatives of the business segment (usually medium and large);
- civil society actors³⁰.

The Center for Countering Disinformation is a working body of the National Security and Defense Council of Ukraine, established in accordance with the decision of the National Security and Defense Council of Ukraine dated March 11, 2021 “On the Creation of the Center for Countering Disinformation”, put into effect by Decree of the President of Ukraine dated March 19, 2021 No. 106³¹. The Center is subordinate to the National Security and Defense Council of Ukraine³². The Center ensures the implementation of measures to counter current and projected

³⁰ Біла книга протидії дезінформації. ГО «Інститут інформаційної безпеки». К., 2022. 62 с. URL: <https://postinfosociety.com/bila-knyga-protydiyi-dezinformacziyi/>

³¹ Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421>

³² Центр протидії дезінформації. URL: <https://cpd.gov.ua/>

threats to national security and national interests of Ukraine in the information sphere, ensure information security of Ukraine, identify and counter disinformation, effectively counter propaganda, destructive information influences and campaigns, and prevent attempts to manipulate public opinion.

In particular, the tasks of the Center include:

detection and counteraction to disinformation, effective counteraction to propaganda, destructive information influences and campaigns, prevention of attempts to manipulate public opinion;

analysis and monitoring of events and phenomena in the information space of Ukraine, the state of information security and the presence of Ukraine in the global information space.

The Center for Strategic Communications was created and operates within the structure of the Ministry of Culture and Information Policy of Ukraine in 2021. The main tasks of this institute include:

- comprehensive analysis and assessment of the external/internal information environment;

- monitoring of relevant narratives with subsequent assessment of the vulnerable group;

- formation of information hygiene in society, raising awareness on countering disinformation;

- support and development of government public communications, including holding workshops, consultations, seminars, meetings, presentations, and other thematic events;

- formation of appropriate conditions for constructive interaction between the state and civil society institutions on the path to joint resistance to hybrid threats.

The Center for Strategic Communications was created as one of the mechanisms for countering disinformation through joint efforts of the state and civil society. The work of the Center is focused on communication counteraction to external threats, in particular, information attacks. The main principles of the Center's activities are constant cooperation with the public sector, the impossibility of political pressure, responsibility and openness.

Information immunity is the ability to identify manipulation, fakes, assess the level of their danger and how they can be prevented. To counter disinformation, it is necessary to develop information immunity in society, increase the level of media culture and media literacy of society.

Ukrainian society must be protected from the destructive influence of disinformation and manipulative information, and the media environment must be socially responsible and function stably. Under such conditions, Ukrainian society will be able to more effectively resist the aggressor state

and remain resilient to a wide range of threats, particularly in the information sphere.

Increasing the level of media culture and media literacy of society will be carried out by performing the following tasks:

- preparing and conducting an educational campaign on media literacy, which will include such components as the development of critical thinking, fact-checking skills and identifying manipulation techniques, familiarization with the most common human rights violations using Internet technologies, etc.;
- creating favorable conditions for the activities of the mass media;
- creating favorable conditions for increasing the level of professional training of media professionals;
- improving legislation in the field of advertising, in particular regarding the liberalization of norms in this area and strengthening responsibility for the broadcast of hidden advertising;
- stimulating the development of socially responsible business among the mass media.

In 2024, Google and Jigsaw, in partnership with the Center for Countering Disinformation, launched a media literacy initiative in Ukraine to combat the spread of disinformation online and increase resilience to common methods of online manipulation³³. The initiative, which uses an approach called "prebunking" (prebunking – literally "preliminary debunking"), is implemented in collaboration with Moonshot and reputable local organizations and experts, in particular the Center for Countering Disinformation, Vox Ukraine, StopFake, detector media, Suspilne and BBC Media Action.

Pre-banking is a communication strategy aimed at increasing resilience to disinformation. Its goal is to help audiences recognize and resist manipulative content, increasing resilience to disinformation in the future.

As a first step of the initiative, implementing partner Moonshot conducted interviews to explore the perspectives of local experts on disinformation and online safety. Moonshot conducted thematic analysis of the interview data to identify common themes of disinformation, manipulation methods, and audiences that may be more vulnerable to or targeted by disinformation. They provided further contextual validation through examples from social media across platforms.

Moonshot identified current and emerging manipulative narratives circulating in Ukraine and identified the following three main manipulation techniques:

³³ Google та Jigsaw у партнерстві з ЦПД запускають ініціативу з медіаграмотності в Україні (24.07.2024). URL: <https://cpd.gov.ua/events/google-ta-jigsaw-u-partnerstvi-z-czpd-zapuskayut-iniciatyvu-z-mediagramotnosti-v-ukrayini/>

Astroturfing – This manipulation tactic involves creating the appearance of social movements through coordinated, inauthentic behavior, often using bots or fake accounts on social media.

Broadest definition: the imitation of a mass public initiative to create the illusion of demand from society. Astroturfing is used both in the field of business for lobbying interests, and in the field of PR, politics and geopolitics (to create the illusion of mass support or condemnation). Its goal, for example, is to force the authorities to listen to the "voice of the people", and convince the people that a certain idea/person / concept "has broad support", so it is worth joining it³⁴. In Ukrainian social media, astroturfing is used to target or artificially suppress or amplify specific content/narratives. This is done through social media, press comments, mass mailings, appeals, and petitions (sometimes influencers and media present astroturfing as a real initiative – consciously or unconsciously).

A key tool in today's astroturfing is the digital technology of bot farms, which simulate a mass popular reaction or initiative. A large number of bot farms are used, which engage in astroturfing on an industrial scale. In Ukraine, astroturfing can have the following manifestations:

1. *Paid protesters*. For example, cases when demonstrators are collected for money for supposedly "voluntary rallies". When journalists try to ask them something, they cannot answer what they are protesting for and against. A subspecies of this astroturfing is activists who can defend their "civic initiative" by force.

2. *Administrative resource astroturfing*. This technique was very popular during the USSR, and is now less common. We are talking about cases when extras were driven out of state-owned enterprises. And a good picture of popular support for the authorities emerged.

3. *Fake sociology astroturfing*. This method is quite simple. Instead of imitating "popular support" for a particular person or idea, you can simply order a fake sociological study that will baselessly give the desired figure.

Emotional manipulation – the provoking of strong emotions such as sadness, hopelessness, anger, and exhaustion in order to prevent critical thinking about a topic. In the Ukrainian context, emotional manipulation is used to exacerbate the psychological exhaustion caused by the military conflict. Manipulations often stimulate intense fear and anger to exacerbate social divisions, as well as to increase existing frustration with Ukrainian institutions and the war effort.

³⁴ Що таке астротурфінг? (25.08.2022). URL: <https://uchoose.uacrisis.org/shho-take-astroturfing/>

Contextualization – the practice of removing information from its original context to create a false or misleading narrative. In Ukraine, fabricated or manipulative news stories spread confusion about which information or news sources are trustworthy. AI-generated deepfakes of prominent politicians and military figures have also targeted citizens with calls to surrender or refuse to donate to the military.

Based on this research and with expert support from local partners, three educational videos were created about these three methods of manipulation that are common in Ukraine. The research and recommendations of experts helped shape the creative idea, based on the findings that the most vulnerable audience is the youth and the older generation, and when evaluating information, people trust relatives and loved ones the most. To reveal these points, the videos use realistic family dialogues in the kitchen with the participation of famous Ukrainian personalities. This familiar environment reflects the place where many families have conversations. By demonstrating conversations about disinformation that cover different relationships and age groups (parents-children, spouses), the videos aim to teach viewers two things: how to recognize manipulation and how to protect their loved ones.

To fully combat the spread of fakes and disinformation, including those that threaten the country's national security, it is necessary to improve the legislation. In this regard, it is useful to study the experience of other countries. It is known that the problem of information security in the era of active development of social networks was once faced by a leading European country – Germany.

Germany is one of the first countries to introduce sanctions at the legislative level for the spread of false information. On June 30, 2017, the German Parliament adopted the Law "On Improving Law Enforcement in Social Networks" (Net Enforcement Act (NetzDG))³⁵. This is also called the Facebook Act. The law aims to combat disinformation (the dissemination of false information about a person that degrades their honor and dignity, harms their business reputation) and incitement to hatred online. The law requires social media platforms with more than 2 million users to establish a transparent procedure for handling complaints about illegal content and requires reporting and documentation. Providers must remove "clearly illegal" content within 24 hours and all illegal content within 7 days of its publication, otherwise they face an administrative fine of up to 50 million euros. Complainants and users must be informed immediately of the decisions taken. Removed content must be kept for at

³⁵ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Social Media Enforcement Improvement Act). URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>

least ten weeks as evidence, and platforms must submit transparency reports on their handling of illegal content every six months.

CONCLUSIONS

The conducted research allowed us to determine the relevance of the problem of disinformation in the media in the context of the war in Ukraine, the main mechanisms of its spread, and to assess modern technologies used to counter information attacks.

Disinformation is a powerful weapon of hybrid warfare, which is actively used to undermine trust in state institutions, destabilize society, and manipulate public opinion. In wartime, its impact becomes even more destructive. Cleaning the information space from fake news and fakes is a prerequisite for overcoming the war and winning.

Modern technologies play a crucial role in combating disinformation. The use of digital technologies will expand the possibilities of timely reporting to law enforcement agencies about offenses, searching for and identifying criminals, and optimizing the process of investigating criminal offenses. Artificial intelligence, automated fact-checking systems, and cybersecurity allow us to detect, analyze, and neutralize information threats. However, these technologies require constant development and adaptation. To effectively combat the spread of false information using innovative digital technologies, it is necessary to use the experience of leading European countries, increase the role of digital tools for detecting and countering disinformation, including in the work of law enforcement agencies, with the involvement of specialized research institutions and leading experts in the field of criminal law, and adapt current legislation to the requirements of the digital age.

Effective countermeasures against disinformation require a comprehensive approach. In addition to technological solutions, it is important to develop the media literacy of the population, improve the legislative framework, and strengthen international cooperation in the field of information security. Ukraine is already demonstrating significant success in combating disinformation, but this process must be continuous and multi-layered. It is important to combine state initiatives, independent media projects, and the active role of civil society. The future of information security depends on the consolidation of efforts – of the state, technology companies, the journalistic community, and society as a whole. Only by combining these resources will the impact of disinformation be minimized and democratic values protected.

SUMMARY

The article is devoted to the study of the problems of disinformation in the language of modern mass media and the protection of human rights in the information space. In times of War, disinformation becomes a powerful tool of information and psychological influence aimed at undermining confidence in state institutions, manipulating public opinion and demoralizing society. This article examines the key mechanisms of disinformation spread in the media, analyzes modern technologies for detecting and countering fakes, including artificial intelligence, fact-checking platforms and cybersecurity methods. The paper focuses on the problem of disinformation in social networks and the information space. Special attention is paid to state initiatives, international experience and strategic approaches to Information Protection of Ukraine. It is concluded that there is a need for an integrated approach that combines technological solutions, legislative measures and the development of media literacy of the population. The author concluded that in order to effectively combat the spread of false information through innovative digital technologies, it is necessary to use the experience of leading European countries, increase the role of digital tools for detecting and countering disinformation, including in the work of law enforcement agencies, with the involvement of specialized research institutions and leading experts in the field of criminal law to adapt the current legislation to the requirements of the digital age.

REFERENCES

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”: Указ Президента України від 28.12.21 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>
2. Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право*. 2023. № 3(46). С. 98–107. URL: <http://il.ippi.org.ua/article/view/287168>
3. Інформаційна безпека: сучасний стан, проблеми та перспективи: збірник матеріалів Міжнародної науково-практичної конференції. Кам’янець-Подільський: Кам’янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf
4. Новий алгоритм пошуку Google на основі AI: чого очікувати (29.10.2023). URL: <https://livepage.ua/blog/the-new-ai-powered-google-search-what-to-expect.html>

5. Аналітичний звіт «російський інформаційний вплив в Африці». URL: <https://cpd.gov.ua/reports/analitchnyj-zvit-rosijskyj-informaczijnij-vplyv-v-afryczj/>

6. Shevchuk Viktor M. Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*. 2020, 27(2). Pp. 170–183.

7. Велика українська юридична енциклопедія : у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків : Право, 2018. 952 с.

8. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008). URL: <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>

9. Як не стати жертвою шахраїв та ворожої пропаганди: кіберполіція про фактчекінг (02 травня 2024 р.). URL: <https://cyberpolice.gov.ua/article/yak-ne-staty-zhertvoyu-shaxrayiv-ta-vorozhoji-propagandy-kiberpolicziya-pro-faktcheking-437/>

10. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: Законопроект України від 19.04.2023 № 9223 / База даних «Законодавство України / ВР України. URL: itd.rada.gov.ua/billInfo/Bills/Card/41788?fbclid=IwAR0RWkqeb5Qfe6H4TPyk_RIKKEZHmqd699_G6ZH0h9ZmxhEwLZ_ZpXM61T0/

11. Аналітичний звіт «російський інформаційний вплив в Африці». URL: <https://cpd.gov.ua/reports/analitchnyj-zvit-rosijskyj-informaczijnij-vplyv-v-afryczj/>

12. Посібник для творців контенту для виявлення та протидії російській пропаганді в нових технологіях. (За підтримки Уряду Великої Британії в рамках проекту «Розуміння штучного інтелекту». 2024. URL: https://ai.instingov.org/assets/guide/AI-Guide_uk.pdf

13. Fact-Checking. URL: <https://reporterslab.org/fact-checking/>

14. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421>

15. Центр протидії дезінформації. URL: <https://cpd.gov.ua/>

16. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 01.09.2017 (Закон

про поліпшення правозастосування в соціальних мережах). URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>.

17. Посібник з верифікації. Центр Європейської Журналістики; Асоціація Видавців (УАВІП). 2014. URL: https://verificationhandbook.com/book_ua18.

18. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: Практичний посібник. Дніпро : ЛІРА, 2017. 133 с.

19. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1>.

20. Ейсмунт В. Інструменти фактчекінгу: як професійно відрізнити брехню від правди. Інститут масової інформації. URL: <https://imi.org.ua/articles/instrumenti-faktcheking-u-yak-profesiyno-vidriznyati-brehnyu-vid-pravdi-i407>

21. Mantis Analytics. URL: <https://mantisanalytics.com/>

22. Фактчек-бот “Перевірка”. URL: https://t.me/perevir_bot

23. Центр протидії дезінформації при РНБО рекомендує новий фактчек-бот "Перевірка" (18.03.2022). URL: <https://imi.org.ua/news/tsentr-protydyi-dezinformatsiyi-pri-rnbo-rekomenduye-novyj-faktchek-bot-perevirka-i44450>

24. Методологія фактчекінгу Гвава Медіа. URL: <https://gwaramedia.com/metodologiya-faktcheking-u-perevirka/>

25. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ в.о. Президента України від 01 травня 2014 р. № 449/2014 URL: <https://zakon.rada.gov.ua/laws/show/449/2014#Text>

26. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента України від 14.09.20 р. № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>

27. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України”: Указ Президента України від 21.03.21 р. № 121/2021. URL: <https://www.president.gov.ua/documents/1212021-37661>

28. Про рішення Ради безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

29. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року “Про Стратегію забезпечення державної безпеки”:

Указ Президента України від 16.02.22 р. № 56/2022. URL: <https://www.president.gov.ua/documents/562022-41377>

30. План реалізації Стратегії кібербезпеки України: Указ Президента України від 01.02.22 р. № 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>

31. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text>

32. Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України від 18.04.23 р. № 328-р. URL: <https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text>

33. Біла книга протидії дезінформації. ГО «Інститут інформаційної безпеки». К., 2022. 62 с. URL: <https://postinfosociety.com/bila-knyga-protydyi-dezinformacziyi/>

34. Центр стратегічних комунікацій. URL: <https://spravdi.gov.ua/>.

35. Google та Jigsaw у партнерстві з ЦПД запускають ініціативу з медіаграмотності в Україні (24.07.2024). URL: <https://cpd.gov.ua/events/google-ta-jigsaw-u-partnerstvi-z-czpd-zapuskayut-initsiatyvu-z-mediagramotnosti-v-ukrayini/> (дата звернення: 01.05.2025).

36. Criminalistics Means and Methods of Combating Ecocide in the Modern Conditions of Military Threats / V. Shevchuk et al. *Journal of Environmental Law & Policy*. 2024. Т. 04, № 03. С. 82–120. URL: <https://doi.org/10.33002/jelp040304> (дата звернення: 01.05.2025).

37. Що таке астротурфінг? (25.08.2022). URL: <https://uchoose.uacrisis.org/shho-take-astroturfing> (дата звернення: 01.05.2025).

Information about the author:
Nehrebetskyi Vladyslav Valerevych,

Ph. D. in Law,
Researcher at Academician Stashis Scientific Research Institute
for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
49, Hryhoriia Skovorody str., Kharkiv, 61002, Ukraine,
Associate Professor at the Department of Criminalistics
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., Kharkiv, 61024, Ukraine