ISSN-L 2664-9969; E-ISSN 2706-5448

UDC 005.21:316.776.23-048.66]:004.8"364"
DOI: 10.15587/2706-5448.2025.327157

Oleksandr Cherep,
Yuliia Kaliuzhna,
Lubomir Mykhailichenko,
Svitlana Markova,
Yevhen Naumenko

FORMATION OF A STRATEGY FOR COUNTERING AND IDENTIFYING AI TECHNOLOGIES IN THE FIGHT AGAINST DISINFORMATION UNDER MARTIAL LAW

The methodological basis of the study is a set of techniques, principles, general theoretical, special, interdisciplinary methods of scientific research. To achieve the set goal, the dialectical method of scientific knowledge was used – to study disinformation in martial law and determine the role of artificial intelligence (AI) in its detection and neutralization. The use of a systemic approach made it possible to determine the features of the spread of disinformation through social networks, traditional media and automated bot farms, for the manipulation of public opinion. The operations research method was used to determine the advantages and disadvantages of AI tools aimed at detecting disinformation. Methods of analogies and comparison – to determine modern methods of combating fake news, including machine learning algorithms, natural language processing and image analysis. It was established that the main problem for increasing the effectiveness of combating disinformation is the implementation of European experience in using AI.

The use of systemic and critical analysis allowed to explore the international experience of using AI tools in the field of information security, their effectiveness in detecting deepfakes and other forms of false content. A comprehensive strategy for countering disinformation in Ukraine is proposed. The proposed strategy, unlike the existing strategy, takes into account the use of artificial intelligence technologies to identify fake content in social networks and news channels, the formation of a special body to analyze digital content and the development of a digital society. The comprehensive strategy, unlike the existing ones, includes the expanded use of AI to monitor the information space, combining automated analysis with human control; the implementation of state initiatives to regulate fake content and increase the level of media literacy of the population. The research results will be useful for scientists, information security experts, journalists and state bodies involved in combating disinformation. The proposed approaches will contribute to strengthening the information protection of Ukraine and reducing the impact of fake news on society.

Keywords: *disinformation, artificial intelligence, fake news, social networks, deepfakes, information security.*

Received: 07.01.2025
Received in revised form: 15.03.2025
Accepted: 06.04.2025
Published: 22.04.2025

How to cite
Cherep, O., Kaliuzhna, Y., Mykhailichenko, L., Markova, S., Naumenko, Y. (2025). Formation of a strategy for countering and identifying AI technologies in the fight against disinformation under martial law. Technology Audit and Production Reserves, 2 (2 (82)), 74–79. https://doi.org/10.15587/2706-5448.2025.327157

1. Introduction

In the context of globalization, the use of AI allows to influence the socio-economic security of the world's states. The use of AI allows to combat disinformation and fake news spread by authoritarian regimes. Therefore, democratic countries around the world are considering the possibility of forming such legislation that will be aimed at the formation of democratic values, compliance with EU legislation on sustainable development of society, preservation of ecosystems and biodiversity. In 2019, Singapore adopted the "Law on Protection from Online Lies and Manipulation", which provides for the protection of society from the spread of false information and manipulation of public opinion [1, 2].

In 2023, EU countries adopted a comprehensive law on the regulation of artificial intelligence (AI), which entered into force on 01.08.2024 [3–6]. EU countries also created a new platform using AI, which will allow to isolate fake information and, by filtering it, prove it to be true [7, 8].

NATO in the context of hybrid warfare also pays much attention to the problematic issues of combating disinformation and fake news through the use of AI technologies [9, 10].

In the era of digital transformation, the global population constantly interacts with information flows, which significantly complicates the process of separating reliable data from content that aims to manipulate public consciousness, especially in conditions of military conflicts. The spread and accessibility of information, on the one hand, provide new opportunities for the exchange of knowledge, but on the other hand, they create risks for the correct perception of reality, which threatens the stability of social structures and the security of the nation. As a result, disinformation poses a significant and wide-ranging threat that can potentially transform the political, economic and cultural structure of any society, thus undermining the fundamental principles of democratic countries. That is why interest in the development of technological tools for automatic verification of information is growing, especially in the changing environment of social networks. Therefore, the topic of preventing the spread of fake information using innovative AI technologies is relevant and timely.

Thus, *the aim of research* is to develop a strategy for combating fakes and disinformation in Ukraine under martial law and the development of AI.

2. Materials and Methods

The object of the study is the process of forming a strategy for countering and identifying AI technologies in the fight against disinformation in martial law. Ukraine has significant scientific potential in the use of AI technologies. It is AI that allows to fight disinformation and fakes. At the same time, to ensure effective counteraction to disinformation, especially in the context of the Russian-Ukrainian war, it is advisable to form a strategy for identifying AI technologies in the fight against fakes. The strategy should be based on a deep analysis of the use of AI.

The issue of using artificial intelligence in the fight against disinformation has become the subject of numerous scientific studies. Researchers focus on automated methods for detecting fake news, in particular the use of deep learning, natural language processing (NLP) and artificial neural network models.

Systematized approaches to detecting deep fakes and noted that modern detection algorithms are based on CNN (Convolutional Neural Networks) and RNN (Recurrent Neural Networks). The authors draw attention to the need to develop hybrid methods that combine algorithmic analysis with human intervention to improve accuracy [11].

According to the study, the most effective models were BERT (Bidirectional Encoder Representations from Transformers) and RoBERTa, which allow identifying false news with an accuracy of over 90 %. At the same time, the authors note that the main problem is the rapid adaptation of disinformation strategies, which complicates the work of the models [12].

The possibility of using autoencoders to detect false content in social networks was also investigated. The results of the analysis showed that autoencoders have significant potential in recognizing hidden manipulations, but their effectiveness depends on the quality of the training data set [13].

The concept of "human-in-the-loop" is also considered as an effective way to combat disinformation. In particular, it has been proposed to combine algorithmic detection of fakes with expert analysis, which allows to significantly reduce the frequency of false positive results [14].

Research emphasizes that the greatest challenges in the fight against disinformation are associated with the rapid development of generative models, in particular GPT-4 and DALL-E. They are capable of creating high-quality content that is visually and textually almost indistinguishable from real data. Among the proposals are regulatory measures and introducing transparency of content generation algorithms [15].

Thus, modern research demonstrates that, despite significant progress in the development of AI tools to combat disinformation, a number of global challenges remain. Important among them are the rapid adaptation of fake technologies, the need for high-quality data sets. It is also advisable to focus on the need to combine automated and human methods of content verification.

The study is based on an interdisciplinary approach that combines methods of content analysis, machine learning and statistical analysis. This study analyzes the problem of disinformation in martial law and the role of artificial intelligence in its detection. In particular, the following scientific methods were used:

– method of analysis of scientific research related to the analysis of the structure of false news in the world;
– generalization method for analyzing the industry structure of cyberattacks by sectors of the Ukrainian economy in martial law;
– comparison for the characteristics of artificial intelligence tools in detecting deepfakes;
– system analysis for the formation of effective artificial intelligence tools for detecting and neutralizing disinformation;
– economic and statistical for studying the structure of social networks by the complexity of detecting false information;
– abstract-logical method, grouping method, statistical methods for analyzing the structure of surveyed Ukrainians by news channels they trust regarding the events of the war in Ukraine;
– graph-analytical method for visualizing the results obtained for the formation of a strategy for combating disinformation in Ukraine in martial law.

To assess the effectiveness of AI tools, existing technologies for analyzing text, images, and videos, including machine learning algorithms and deep neural networks, were considered. International experience in combating disinformation and the specifics of using AI in Ukraine's information security were also examined.

3. Results and Discussion

The development of digital technologies and the globalization of the information space have significantly exacerbated the problem of disinformation in the world. Manipulative content is used as a tool to influence public opinion, the political situation and economic processes. In Europe and North America, the problem of disinformation remains relevant, especially in the context of election campaigns and pandemic crises. In the EU countries, regulatory mechanisms, such as the Digital Services Act (DSA), are in place to combat the spread of fake news, but even these measures do not guarantee complete control over disinformation flows. At the same time, in the USA, the Meta and Google platforms have introduced algorithms based on artificial intelligence to detect false news, which has reduced the amount of disinformation. A key feature of the global information space is the active use of artificial intelligence as a tool both for combating disinformation and for its creation. For example, the FactCheck.org, Snopes and ClaimBuster platforms use natural language processing (NLP) algorithms to automatically detect potentially false news. However, at the same time, machine learning methods are also used to generate fake content, including synthesized video and audio, which complicates the process of verifying information.

Fig. 1 shows the structure of world news in which false information was detected.

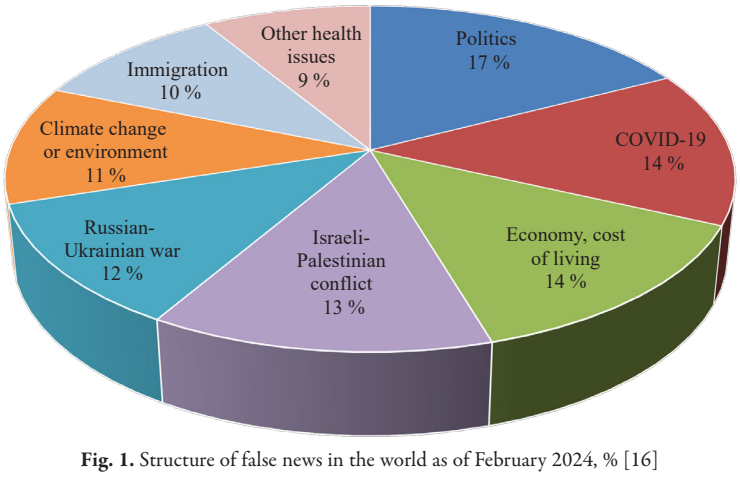

Fig. 1. Structure of false news in the world as of February 2024, % [16]

The Russian-Ukrainian war is one of the vivid examples of the active dissemination of false information by the enemy through social networks and other channels, which indicates the relevance of using modern technologies to identify such information. As can be seen from Fig. 1, the share of false news about the war in Ukraine is 12 %, which indicates significant propaganda by the aggressor and the dissemination of false information. In addition, a large part of false information actively circulates through social media, which has become the main

ISSN-L 2664-9969; E-ISSN 2706-5448

channel for the dissemination of disinformation materials. Social platforms are publicly available and have a huge audience, which provides them with great power to influence public opinion. The ease of creating and distributing fake news without the need for its reliable verification allows manipulators to effectively implement information influence strategies. The lack of control mechanisms on some platforms contributes to the widespread dissemination of false information, making it much more difficult to identify and neutralize it. In this regard, the fight against information attacks requires the development and implementation of effective methods for the rapid detection of fake news, which will contribute to increasing the level of information security in Ukraine.

Fig. 2 shows the main sectors of the Ukrainian economy that were targeted by cyberattacks during martial law. As shown in Fig. 2, the largest targets of cyberattacks were critical infrastructure facilities and government portals, with the main source of such attacks being located in the territory of the aggressor country.

In this regard, there is a need to implement effective artificial intelligence tools to detect and neutralize disinformation, which often acts as a key catalyst for cyberattacks aimed at destabilizing the information space and undermining national security.

Fig. 3 shows a rating of social networks in which it is most difficult to distinguish truth from fakes.

Fig. 3 shows that social networks such as TikTok and X are the most difficult platforms for determining the reliability of news content. As for Facebook and Instagram, an almost similar situation can be observed in them, since 21 % and 20 % of respondents found it difficult to recognize the truthfulness of the content.

Fig. 4 shows the structure of the surveyed Ukrainians by news channels that they trust regarding the events of the war in Ukraine. Analyzing the data in Fig. 3, it should be noted that 97 % of Ukrainians trust domestic news channels and the information broadcast on them. The highest level of trust is given to 1+1 and Inter with a share of 33 % and 26 %, respectively.

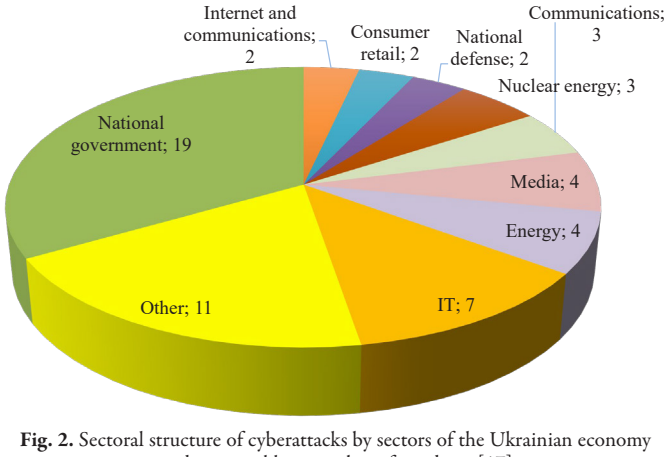

Fig. 2. Sectoral structure of cyberattacks by sectors of the Ukrainian economy under martial law, number of incidents [17]

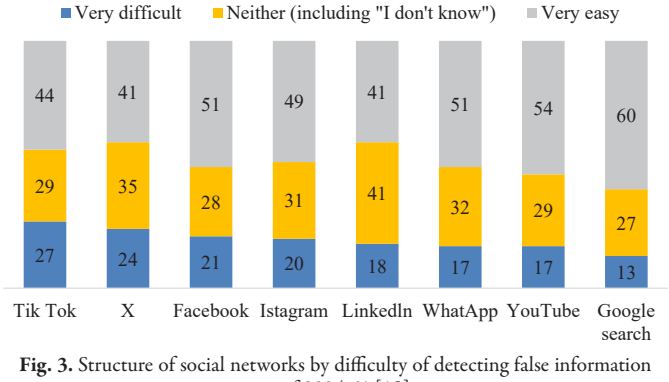

Fig. 3. Structure of social networks by difficulty of detecting false information as of 2024, % [18]

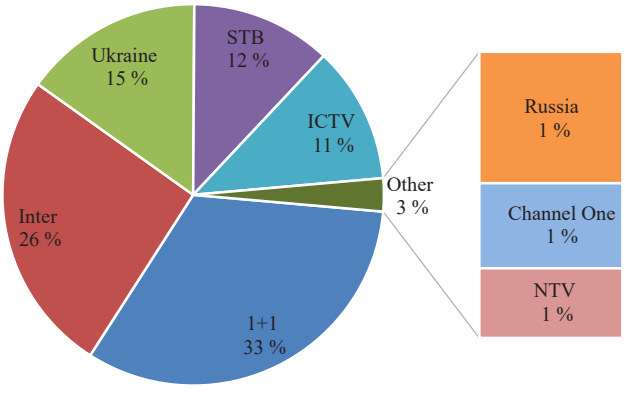

Fig. 4. Share of trust of Ukrainians in news channels regarding events in the war [19]

That is why the use of artificial intelligence tools aimed at identifying and detecting disinformation is effective. Based on the analysis of scientific literature and studies directly devoted to the automatic detection of disinformation using AI technologies, it was found that there are different approaches to its application [11, 12]. Some authors see the automatic identification of disinformation as a problem of detecting anomalies in social networks, using an autoencoder as a method of unsupervised learning [19], others use Bayesian statistics to calculate the veracity of news and trust in their authors [14]. Nevertheless, most studies use a mixed approach, which implies the use of both artificial intelligence technologies and human analysis.

Therefore, machine learning algorithms play an important role in the fight against disinformation, in particular those used for text analysis and assessment of the reliability of information. One of the most effective approaches is text classification, where algorithms such as naive Bayesian classifiers, support vector machines (SVMs), and deep neural networks are used to identify fake news, manipulative texts, or misrepresented facts.

A naive Bayesian classifier, for example, uses probabilistic models to evaluate the words that appear in a text and their relationships to determine whether the text is authentic or suspicious. The support vector machine allows for efficient classification of more complex text sets, where it is necessary to find hyperplanes that maximize the distance between categories. Deep neural networks such as BERT and GPT can understand context and distinguish fake news, taking into account even the smallest nuances in language structures.

The second important step is to assess the reliability of the information mentioned in the news. Machine learning algorithms can verify facts by comparing them with existing databases and official sources. In particular, AI-powered fact-checking tools can automatically match claims with verified data, significantly reducing the risk of misinformation spreading. Combined with entity recognition (NER) methods that automatically detect names, places, and events, these algorithms can identify and verify key elements of text.

These algorithms can work in real time, allowing for timely detection of news and social media posts containing disinformation. For example, an algorithm that analyzes social media messages can instantly warn users or news editors about possible false information. This ensures a quick response and reduces the risks of spreading manipulation.

In addition, the integration of such algorithms into media and social media monitoring systems allows for the creation of automated platforms for detecting and combating disinformation in real time. AI algorithms can be integrated into news platforms, where they can analyze publications, identify potentially fake news,

and provide editors with recommendations for fact-checking before publication. This not only improves the effectiveness of the fight against fake news, but also reduces the burden on journalists, who usually have to manually check each statement for veracity.

The use of machine learning can also improve recommendation algorithms on social networks, limiting the spread of false information. Algorithms that detect manipulation can filter out false messages that users may spread through personal profiles. This is especially important in an environment where disinformation can quickly go viral due to algorithms that assess the popularity of content based on engagement.

Another important aspect is to educate users and create support systems for critical thinking, allowing them to better understand and evaluate the reliability of the information they consume. AI can serve as an auxiliary tool, providing users with verified information and warning about potential manipulation.

Table 1 lists artificial intelligence tools that can detect deepfakes used in military conflicts to misinform society.

Therefore, the above tools are effective tools for identifying deepfakes and detecting false content. The issue of countering disinformation using artificial intelligence is extremely important, but it is significantly complicated by the rapid development of fake generation technologies, as both means of countering disinformation and programs for creating fake news and content are being improved [21].

Table 2 lists the main advantages and disadvantages of artificial intelligence tools aimed at detecting disinformation.

The tools listed in Table 2 are effective and convenient to use and help to quickly detect fake news.

In the context of martial law and constant hostile propaganda, Ukrainian IT developers have created AI-based platforms [22] that effectively help detect destructive information influence campaigns at an early stage. Their capabilities are based on the CommSecure and CIB Guard software. CommSecure allows to detect certain narratives in messages on social networks and communities, for example, public groups in messengers. This ensures rapid detection and analysis of potentially dangerous information flows. CIB Guard specializes in analyzing users' public pages, detecting bots, and determining whether they are acting in a coordinated manner. This approach allows to quickly recognize coordinated campaigns that may be aimed at manipulating public opinion and spreading disinformation.

Below is a general strategy for combating disinformation in the context of AI development and war (Fig. 5). In the context of the Russian-Ukrainian war and the active use of information technologies for manipulation, a general strategy for combating disinformation in Ukraine is proposed, which integrates modern artificial intelligence (AI) methods for automated detection and neutralization of false content. The strategy is aimed at effective monitoring of television channels and social networks to ensure timely detection of fake news, manipulations, and propaganda that can influence public opinion.

The goal of the existing information security strategy in Ukraine (2021) is to ensure the information security of Ukraine, aimed at protecting the vital interests of citizens, society and the state from internal and external threats, ensuring the protection of national sovereignty and territorial integrity of Ukraine, maintaining social and political stability, ensuring the rights and freedoms of every citizen [23, 24].

Table 1

Characteristics of artificial intelligence tools for detecting deepfakes

Tool	Features
Deepware Scaner	A fake detection platform that aims to prevent the spread of synthetic media and disinformation. To do this, the platform detects AI-generated manipulations of human faces in videos uploaded to platforms such as YouTube, Facebook, and Twitter
DuckDuckGoose	A deepfake detection tool designed to protect organizations from potential threats related to media manipulation, including images, videos, audio, and text. This comprehensive set of verification tools not only confirms whether the content is fake, but also provides clear explanations of how the manipulation was detected, giving the user a high level of confidence in the accuracy of fake detection
Google SynthID	A watermarking tool for AI-generated content. SynthID allows to embed digital watermarks into AI-generated images, videos, and audio files, making the identification process easier
Intel FakeCatcher	A product designed to detect and flag fraudulent videos. FakeCatcher operates via a web-based platform on a server using both Intel software and hardware
Sensity	An AI-based solution designed to effectively detect deep fake content such as face swapping, audio manipulation, and AI-generated images

Note: based on [20]

Table 2

Advantages and disadvantages of artificial intelligence tools in detecting false information

Tool	Features	Advantages	Disadvantages
RevEye	A detection tool that analyzes web pages and social media posts to detect image manipulation, edited films, and misleading headlines	Effective image analysis for authenticity. Convenient interface allows for quick verification	Limited capabilities for detecting manipulation. Reliance on visual cues can lead to false positives
TruthBird	A disinformation detection tool that scrapes text, images, and videos from social media, message boards, and websites	An improved algorithm reveals nuances of disinformation. Real-time monitoring complements timely verification of truthfulness	Resource-intensive, impacts machine performance. Vulnerable to procedures that evolve to create misleading content
BotSlayer	BotSlayer offers disinformation detection tools that instantly display bot scores on Twitter and Facebook profiles	Reliable detection of computerized pastime in social networks. Customizable filters for individual analysis	May generate false positives in dynamic online environments. Exhausts resources during large-scale monitoring
SpotDeep Fakes	SpotDeepFakes determines how likely an image or video is to be altered	Deep learning of new trends enhances deep identification of fakes. Constant updates increase adaptability to new technologies	Limited effectiveness in combating fairly complex counterfeits. Resource-intensive processing for high-resolution content
CredEye	A fake news detection tool that analyzes sentiment and emotions, verifies sources, and looks for logical errors and biases	Comprehensive cross-platform reliability diagnostics. Integration with information sources ensures accuracy in real time	Possible difficulty in localized content verification. Potential lag in detecting unexpectedly spreading disinformation

ISSN-L 2664-9969; E-ISSN 2706-5448

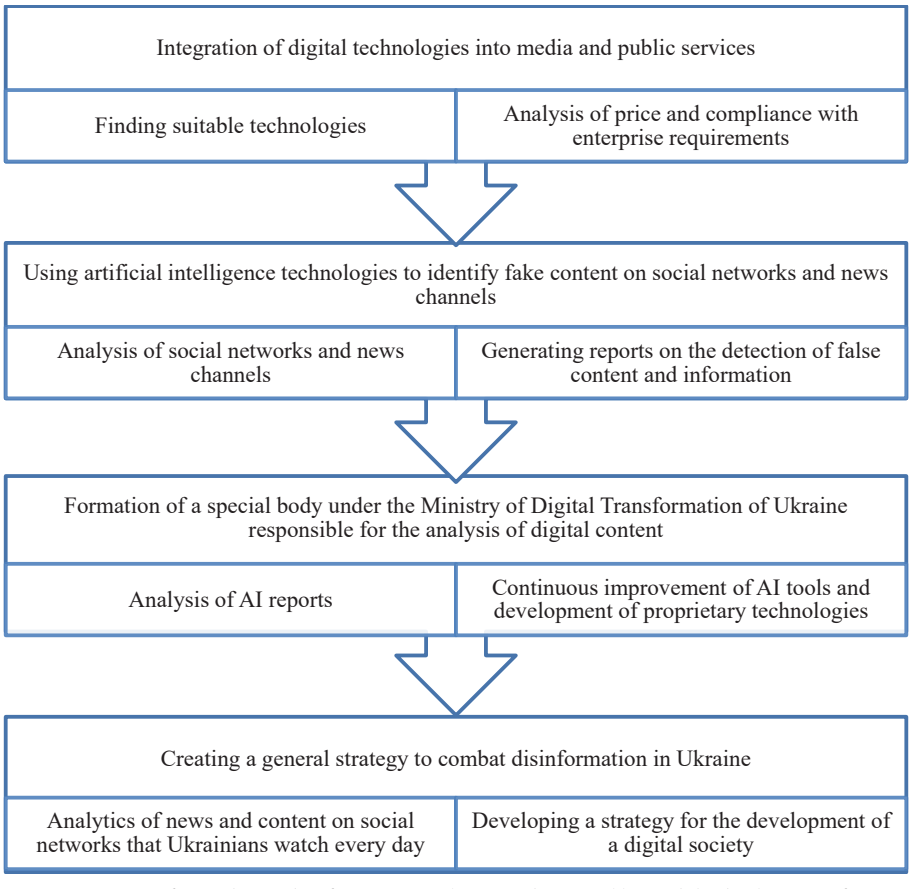

Fig. 5. Strategy for combating disinformation in Ukraine under martial law and the development of AI

The proposed strategy (Fig. 5) differs significantly from the one developed and approved by the National Security Council of Ukraine, as it provides for the integration of digital technologies in the media and civil service. Also, unlike the existing strategy, it provides for the search for relevant AI technologies, analysis of social networks and news channels, and generation of reports on the detection of false content and information. Unlike the existing strategy, it proposes the constant improvement of AI tools and the development of its own technologies and analytics of news and content on social networks that Ukrainians watch every day.

Thus, the developed digital strategy for combating disinformation in Ukraine is aimed at identifying and neutralizing false content distributed through television channels and social networks. Its main goal is to prevent destructive information influence, in particular in the context of war and other socially significant events. Since information attacks are an integral part of modern hybrid wars, effective counteraction to disinformation is a critically important element of ensuring national security. Ukraine must protect its population not only from physical threats, such as missile strikes, but also from information manipulations aimed at undermining public trust, destabilizing society and distorting the real state of events.

Discussion. The role of artificial intelligence in combating disinformation has significantly increased over the past decade, as electronic algorithms are able to "learn" from large volumes of data, identifying characteristic patterns inherent in disinformation materials. These algorithms use the detected patterns to automatically assess the likely reliability of content, in particular to identify elements that may indicate manipulation or falsification of information, thereby ensuring effective detection and filtering of false messages. That is why the use of artificial intelligence technologies in identifying false information and developing tools to effectively counteract it is relevant.

The impact of martial law conditions. It is especially important to identify false information and form a strategy to counter disinformation in the conditions of the Russian-Ukrainian war. The enemy, having a significant information array of data, uses it to intimidate the civilian population and distort the facts surrounding the military of the Armed Forces of Ukraine. The proposed strategy for combating disinformation in Ukraine allows using AI to identify fake content in social networks and news channels. In conditions of martial law, such a strategy is aimed at developing the necessary digital competencies among Ukrainians to counter disinformation.

The limitations of the strategy for combating disinformation in Ukraine under martial law and the development of AI are the integration of digital technologies in the media and public services. During the Russian-Ukrainian war, such integration is not productive, so it does not allow analyzing digital content to combat disinformation.

Prospects for further research include the development of hybrid models that combine AI algorithms with crowdsourcing methods of information verification, as well as assessing the effectiveness of different approaches in real-world information warfare. An important direction is also the study of the moral and ethical aspects of using AI in the process of content moderation and the possible impact of automatic algorithms on freedom of speech.

4. Conclusions

The role of artificial intelligence in combating disinformation under martial law was analyzed. It was found that deep learning, natural language processing, and anomaly recognition technologies play a key role in detecting fake news, deepfakes, and manipulative content.

The study confirmed that in Ukraine, as in other countries, social networks remain the main channel for the spread of disinformation, which makes automated analysis systems particularly relevant. The most difficult task is to combat new types of falsifications generated by neural networks, as they are of high quality and quickly adapt to detection algorithms.

The proposed strategy for countering disinformation in Ukraine includes three main areas. The first area involves expanding the use of AI tools for monitoring and analyzing information flows, which will allow detecting false content and information. The second area is associated with strengthening human control through the integration of expert assessments into the detection system, which provides guarantees of obtaining truthful information. The third direction is aimed at introducing state initiatives to increase the information literacy of the population and the implementation of stricter regulatory measures, which is extremely important in wartime.

Conflict of interest

The authors declare that they have no conflict of interest regarding this research, including financial, personal, authorship or other, which could affect the research and its results presented in this article.

Financing

The research was conducted without financial support.

Data availability

The manuscript has no linked data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. *Act is the Protection from Online Falsehoods and Manipulation* (2019). Available at: https://sso.agc.gov.sg/Act/POFMA2019?ProvIds=P11-#pr1-
2. Petriv, O. (2019). Shtuchnyi intelekt i dipfeiky: yak krainy reahuiut na zahrozy. *Tsentr demokratii ta verkhovenstva prava.* Available at: https://cedem.org.ua/analytics/shtuchnyi-intelekt-i-dipfeiky/
3. Saakov, V., Kropman, V. (2024). *Yevroparlament skhvalyv zakon pro shtuchnyi intelekt.* Available at: https://www.dw.com/uk/evroparlament-shvaliv-zakon-pro-stucnij-intelekt/a-68516616
4. Pershyi u sviti zakon pro ShI nabuv chynnosti u YeS (2024). *UNN.* Available at: https://unn.ua/news/pershyi-u-sviti-zakon-pro-shi-nabuv-chynnosti-u-yes
5. *European Council meeting (19 and 20 March 2015) – Conclusions.* Available at: http://www.eesc.europa.eu/resources/docs/european-council-conclusions-19-20-march-2015-en.pdf
6. IeS zapustyt novu platformu dlia borotby z dezinformatsiieiu Rosii ta Kytaiu (2023). *Yevropeiska pravda.* Available at: https://www.eurointegration.com.ua/news/2023/02/7/7155675/
7. Holub, R. (2022). *Onovlennia kodeksu YeS shchodo borotby z dezinformatsiieiu: osnovni polozhennia.* Available at: https://jurliga.ligazakon.net/news/212519_onovlennya-kodeksu-s-shchodo-borotbi-z-deznformatsyu-osnovnpolozhennya
8. Vaskiv, O. (2023). *Bloomberg: Yevrosoiuz vyznav sotsmerezhu X naibilshym dzherelom dezinformatsii.* Available at: https://suspilne.media/580681-bloomberg-evrosouz-viznav-socmerezu-x-najbilsim-dzerelom-dezinformacii/
9. *Pidkhid NATO u haluzi borotby z informatsiinymy zahrozamy* (2025). Available at: https://www.nato.int/cps/uk/natohq/topics_219728.htm
10. *NATO vpershe zaiavylo pro zanepokoiennia dezinformatsiieiu iz zastosuvanniam shtuchnoho intelektu* (2024). Henshtab ZSU. Available at: https://armyinform.com.ua/2024/07/13/nato-vpershe-zayavyla-pro-zanepokoyennya-dezinformacziyeyu-iz-zastosuvannyam-shtuchnogo-intelektu-genshtab-zsu/
11. Dagar, D., Vishwakarma, D. K. (2022). A literature review and perspectives in deepfakes: generation, detection, and applications. *International Journal of Multimedia Information Retrieval, 11 (3),* 219–289. https://doi.org/10.1007/s13735-022-00241-w
12. Zhang, X., Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management, 57 (2),* 102025. https://doi.org/10.1016/j.ipm.2019.03.004
13. Li, D., Guo, H., Wang, Z., Zheng, Z. (2021). Unsupervised fake news detection based on autoencoder. *IEEE Access, 9,* 29356–29365. https://doi.org/10.1109/ACCESS.2021.3058809
14. Yang, J., Vega-Oliveros, D., Seibt, T., Rocha, A. (2021). Scalable fact-checking with human-in-the-loop. *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS).* https://doi.org/10.1109/WIFS53200.2021.9648388
15. Mitchell, T., Martin, E. (2023). Challenges of combating disinformation in the era of generative AI. *Journal of Artificial Intelligence and Society, 15 (4),* 527–542.
16. *News consumers who saw false or misleading information about key topics in the last week worldwide as of February 2024.* Available at: https://www.statista.com/statistics/1317019/false-information-topics-worldwide/ Last accessed: 14.01.2025
17. *Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* Digital Security Unit. (2022). Available at: https://complexdiscovery.com/russian-cyberattack-activity-in-ukraine-a-special-report-from-microsoft/
18. Overview and key findings of the 2024 Digital News Report (2024). *Reuters.* Available at: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/dnr-executive-summary Last accessed: 14.01.2025
19. *Disinformation Resilience in Central and Eastern Europe.* Available at: https://prismua.org/en/dri-cee/ Last accessed: 14.01.2025
20. Khandelwal, N. (2024). *10 Top AI Deepfake Detector Tools for 2024 & Beyond.* Available at: https://vlinkinfo.com/blog/top-ai-deepfake-detector-tools/ Last accessed: 16.01.2025
21. *Center for AI Safety. Statement on AI risk*. Available at: https://www.safe.ai/work/statement-on-ai-risk Last accessed: 17.01.2025
22. Osavul. *AI-powered platform for information environment assessment.* Available at: https://www.osavul.cloud/ Last accessed: 17.01.2025
23. *Pro Stratehiiu informatsiinoi bezpeky* (2021). Rishennia. Rada natsionalnoi bezpeky i oborony Ukrainy 15.10.2021. Available at: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text
24. Safarov, A. (2021). *Analiz «Stratehii informatsiinoi bezpeky» v porivnianni z chynnoiu Doktrynoiu informatsiinoi bezpeky.* Available at: https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852

✉ ***Oleksandr Cherep,*** *Doctor of Economic Sciences, Professor, Department of Staff and Marketing Management, Zaporizhzhia National University, Zaporizhzhia, Ukraine, e-mail: cherep2508@gmail.com, ORCID: https://orcid.org/0000-0002-3098-0105*

Yuliia Kaliuzhna, *PhD, Associate Professor, Department of Staff and Marketing Management, Zaporizhzhia National University, Zaporizhzhia, Ukraine, ORCID: https://orcid.org/0000-0002-3335-6551*

Lubomir Mykhailichenko, *PhD Student, Zaporizhzhia National University, Zaporizhzhia, Ukraine, ORCID: https://orcid.org/0000-0003-3545-0805*

Svitlana Markova, *Doctor of Economic Sciences, Professor, Department of Business Administration and Foreign Economic Activity Management, Zaporizhzhia National University, Zaporizhzhia, Ukraine, ORCID: https://orcid.org/0000-0003-0675-0235*

Yevhen Naumenko, *PhD Student, Zaporizhzhia National University, Zaporizhzhia, Ukraine, ORCID: https://orcid.org/0009-0004-9111-8617*

✉ *Corresponding author*