

# NEGATIVE IMPACTS IN THE ONLINE ENVIRONMENT: EFFECTIVE STRATEGIES AND MEASURES FOR COUNTERACTION

Petrenko Svitlana

DOI: <https://doi.org/10.61345/1339-7915.2025.2.16>

**Annotation.** The significance of legal frameworks in ensuring data security and regulating behavior in the digital environment with a particular focus on cyberbullying and hate speech is explored in the study. It emphasizes the need to strike a balance between technological innovation, the evolving nature of cyber threats, and the protection of fundamental human rights. The study also highlights the crucial role of education and awareness-raising initiatives in fostering secure digital space.

Criminal law mechanisms for addressing cyber threats and online abuse are grounded in legislative frameworks that define cybercrimes and establish corresponding criminal liabilities. These mechanisms encompass a broad spectrum of offenses, including unauthorized access to data, cyber fraud, the distribution of malicious software, and the dissemination of hate speech in digital environments. Effective enforcement requires the identification, prosecution, and sanctioning of offenders, which in turn depends on coordinated efforts among law enforcement agencies and the efficient operation of the judicial system.

Legal provisions play a crucial role in addressing and mitigating digital violations. They encompass the right to challenge false information, protect personal data, seek compensation for harm caused by cybercrimes, and exercise the right of reply in cases involving defamatory or evaluative content. These legal safeguards empower victims of cyberbullying and other forms of online abuse to assert their rights through judicial mechanisms. The effective implementation of such measures relies on a well-defined legal framework and increased public awareness of individual rights and the available channels for legal recourse.

This analysis underscores the need for a comprehensive strategy that integrates legal instruments with educational initiatives aimed at promoting responsible digital behavior and cyber hygiene. Moreover, it highlights the imperative of continuously updating legal frameworks to keep pace with the dynamic and rapidly evolving challenges of the digital environment.

**Key words:** cyber hygiene, psychological impact, online abuse, cybercrime, cyber offenses, hate speech.

## 1. Problem Statement.

In the contemporary context, where digital technologies are integrated into everyday life, the imperative to maintain effective cyber hygiene and safeguard individual rights online has become increasingly urgent. As digital interactions play a growing role in shaping personal and social experiences, they simultaneously give rise to significant psychological risks, including cyberbullying, the spread of misinformation, hate speech, and various forms of digital exploitation.

Within this environment, legal frameworks serve a vital role in regulating conduct in the digital sphere. The effective enforcement of legal protections is essential not only for mitigating psychological harm but also for ensuring individuals are shielded from a broad array of online misconduct. However, the rapid and continuous evolution of digital technologies raises pressing


concerns about the sufficiency of current legal measures in responding to the complex challenges of the digital age.

This study offers a critical examination of Ukrainian legislation as a protective mechanism against cyberbullying, disinformation, and other forms of digital manipulation. Special attention is given to existing legal instruments aimed at preventing and responding to online abuse, alongside an assessment of the ongoing need for legislative refinement and modernization. The study concludes with practical recommendations for the further development of Ukraine's legal system to more effectively address the demands of the digital environment and ensure the robust protection of human rights and fundamental freedoms in the digital era.

## 2. Analysis of scientific publications and literature.

In the research conducted by Y. V. Bilyavska and Y. I. Shestak, the relationship between cybersecurity and cyber hygiene is analyzed within the context of contemporary digital technologies [1, p. 47–59]. B.I. Drishliuk examines the concept of abuse of civil rights, which holds significant importance in the context of cyber hygiene [2, p. 242–246]. O.O. Klymchuk dedicates his work to analyzing the legal foundations of cybersecurity in the United Kingdom [3, p. 87–90]. I.M. Kozubtsov, V.P. Sameliuk, and M.P. Yavich provide an overview of various approaches to defining cyber hygiene [4, p. 301–304]. Z. Sverdyk focuses on issues related to cybersecurity and cyber defense, which are particularly relevant to Ukrainian society [5, p. 175–188]. I.M. Sopilko discusses the specific legal measures for countering cyber threats [6, p. 105–110]. V. Subotka and N.V. Medvedenko examine the legal regulation of cybersecurity and identify the key stakeholders involved in Ukraine [7, p. 19–22]. V.O. Tishchenko and Y.S. Lohvynenko analyze the legal principles for ensuring cybersecurity during martial law [8, p. 71–73]. Finally, O.V. Shagaka explores issues related to compensation for damages resulting from the abuse of rights in the context of online contract formation [9, p. 180].

The relevance of this topic stems from the urgent need to develop effective legal mechanisms and strategies for protecting individuals from cyber threats and abuses in the digital environment. As digital technologies continue to advance, the establishment of robust and adaptive legal safeguards against emerging risks has become a pressing concern for both policymakers and society as a whole.

 **3. The primary aim** of this research is to analyze and formulate comprehensive legal frameworks for the protection of individuals in cyberspace. This entails a critical evaluation of existing legislative structures and the formulation of targeted reforms to more effectively address the evolving and multifaceted nature of cyber threats.

## 4. Presentation of the main provisions.

The concept of “cyber hygiene” refers to the set of actions undertaken to prevent cyberattacks, safeguard personal and organizational data, and maintain the confidentiality of information. It encompasses the set of measures and practices adopted by individuals, organizations, and society to ensure security and protection within the digital environment. Effective cyber hygiene involves routine software updates, the use of reputable antivirus programs, the creation of strong and unique passwords, prudent engagement on social media platforms, and ongoing user education about potential cyber threats.

The legal dimensions of cyber hygiene encompass a range of regulations and standards aimed at protecting digital information systems and data, as well as safeguarding individuals' civil rights and interests in the digital sphere. These legal frameworks include legislation on cybersecurity, personal data protection, copyright, and intellectual property rights, all of which are essential for maintaining order and accountability in the online environment. In addition, they address legal provisions concerning liability for cybercrimes such as hacking, phishing, the dissemination of malicious software, and other forms of cyberattacks. Collectively, these regulations establish a comprehensive

legal foundation for ensuring cybersecurity and protecting users from unlawful or harmful online activities.

Cyber offenses in the digital realm refer to actions or omissions that violate established legal norms through the use or misuse of digital technologies and information systems. Such offenses may include unauthorized access to computer networks, the distribution of malware, cyber fraud, intellectual property violations, phishing schemes, cyberbullying, and other manifestations of online abuse. The subsequent discussion characterizes the various forms of cyber misconduct and explores the legal mechanisms available to combat these threats. Depending on the specific circumstances, such actions may give rise to criminal, administrative, or civil liability.

**Cyber fraud** constitutes a category of criminal activity that involves the use of computer and network technologies to deceive individuals or organizations for the unlawful acquisition of assets. The societal threat posed by cyber fraud is significant, as it undermines public trust in digital systems, results in substantial financial losses for both individuals and institutions, and compromises broader cybersecurity infrastructures. These activities can have far-reaching consequences, including economic instability and threats to personal safety.

One of the most prevalent forms of cyber fraud is **phishing**, which has evolved in parallel with the expansion of internet technologies. Phishing typically involves fraudulent emails, messages, or websites that are crafted to trick users into disclosing sensitive information such as login credentials, personal identification numbers, or banking details. In Ukraine, as in many other countries, phishing remains a pervasive form of cybercrime and is used to gain unauthorized access to financial accounts.

Another common method of cyber fraud is **skimming**, which entails the covert installation of unauthorized devices on ATMs or point-of-sale terminals to extract information from the magnetic stripes of payment cards. These devices are often designed to be inconspicuous to users. For example, skimming equipment may be attached to ATM card slots to read card data, while miniature cameras or keypad overlays are used to capture PIN codes. The harvested data is subsequently used to produce counterfeit cards and facilitate unauthorized transactions.

Additionally, cybercriminals often employ **trust-building tactics**, whereby they establish a relationship of credibility and emotional rapport with potential victims before executing the fraud. This psychological manipulation enhances the likelihood of success by lowering the victims' suspicion and increasing their willingness to comply with fraudulent requests.

Bank account fraud involves schemes in which perpetrators gain unauthorized access to individuals' financial accounts, often through the deployment of malicious software or the exploitation of banking data obtained via phishing attacks. These methods enable fraudsters to bypass security protocols and conduct unauthorized transactions, resulting in financial losses for the account holders.

Investment cyber fraud refers to deceptive practices associated with online investment platforms, wherein victims are enticed by promises of unusually high returns on investments in digital assets. In many cases, individuals are persuaded to deposit funds into seemingly legitimate platforms, only to lose their investments once the fraudsters abscond with the money. A common tactic includes the creation of counterfeit websites that closely resemble authentic investment services, thereby deceiving users into transferring funds under false pretenses. Promoted opportunities may involve cryptocurrencies, startup ventures, or other high-risk digital assets.

Another widespread variant is the pyramid scheme, in which returns to earlier investors are paid using the capital of newer participants. This structure creates the illusion of profitability and sustainability, encouraging further investment. However, such schemes are inherently unstable and inevitably collapse, leaving the majority of participants with substantial financial losses.

The actions described above may constitute criminal offenses if they exhibit societal danger, defined as the potential or actual capacity to inflict significant harm on legally protected interests. Consequently, under specific circumstances, such actions may be classified under Article 190 of the Criminal Code of Ukraine (hereinafter referred to as the CC of Ukraine) as fraud. Fraud is characterized by the unlawful acquisition of another person's property or rights to property through deception or abuse of trust.

To classify cyber fraud within the framework of the relevant provisions of the Criminal Code of Ukraine, it is essential to analyze the specific formulation of the objective element of the offense as outlined in Article 190 of the CC of Ukraine. A distinguishing characteristic of fraud is that its object encompasses not only tangible assets but also rights pertaining to those assets. Such rights are documented in various legal instruments, including shares, powers of attorney for property management, debt agreements, wills, and others. A comprehensive description of property rights is provided in the general provisions of this section.

On the other hand, the objective element of fraud is characterized by the unlawful acquisition of property or the illicit obtaining of rights to property through deception or abuse of trust. As a consequence of such fraudulent behavior, the victim—typically the owner or custodian of the property—voluntarily transfers ownership or rights to the offender. Within the context of this study, it is important to highlight that the victim's voluntary decision and active participation in the transfer of property constitute essential distinguishing features of fraud, differentiating it from theft and other property-related offenses.

Accordingly, if cyber fraud involves demands for the transfer of property or the execution of property-related actions under threats of violence directed at the victim and/or their close relatives; threats to violate their rights, freedoms, or legitimate interests; threats of destruction or damage to their property or to property entrusted to them; or threats to disclose confidential information concerning the victim or their relatives, such conduct should be classified under Article 189 of the Criminal Code of Ukraine.

Although fraud shares certain characteristics with extortion—particularly the active involvement of the victim in the unlawful transfer of property—it fundamentally differs with respect to the victim's motivation. In cases of fraud, the victim is deceived into believing that they are acting voluntarily and in their own best interest, despite being misled about the legality or legitimacy of the property transfer or the associated rights. This apparent voluntariness is, in fact, illusory, as it is found on deception.

In circumstances where the victim, due to factors such as age, cognitive or physical impairments, or particular situational conditions, is unable to fully comprehend or control their actions, the transfer of property or rights resulting from cyber fraud cannot be regarded as genuinely voluntary. The exploitation of such vulnerabilities to acquire property can be classified as theft. Furthermore, the acquisition of rights to property under these conditions can be deemed an invalid or voidable transaction in accordance with Articles 222–226 of the Civil Code of Ukraine (Law No. 435-IV, January 16, 2003).

Having examined cyber fraud as a significant consequence of inadequate cyber hygiene and the legal frameworks available to combat it, this study now turns to another increasingly pervasive digital threat: **cyberbullying**. Cyberbullying constitutes a form of harassment or intimidation executed through digital communication platforms such as social media, messaging applications, online gaming environments, forums, and email. It encompasses a spectrum of aggressive behaviors, including the dissemination of false information, offensive or derogatory remarks, threats, and acts of public humiliation.

What distinguishes cyberbullying from traditional forms of bullying is its potential for anonymity and rapid dissemination, which enable it to reach a broad and diverse audience. These characteristics render cyberbullying particularly harmful, often resulting in significant and enduring psychological trauma for victims, manifested through symptoms such as stress, anxiety, and depression.

The advent of modern communication technologies has endowed cyberbullying with unique attributes absent in conventional bullying. In traditional contexts, victims typically identify their aggressors and may respond verbally or physically. Conversely, the virtual environment frequently conceals perpetrators' identities, complicating detection and accountability. This anonymity often allows cyberbullying to persist unchecked, thereby hindering efforts by legal and judicial institutions to effectively address and remediate such violations.

The anonymity of individuals who engage in cyberbullying, combined with the ease of deleting or altering online communications, significantly complicates efforts to protect victims' rights. Despite

these challenges, Ukrainian legislation provides a robust legal framework for addressing such conduct.

The legal definition of cyberbullying in Ukraine was established by the Law of Ukraine “On Amendments to Certain Legislative Acts of Ukraine Concerning Counteraction to Bullying,” adopted on December 18, 2018. Pursuant to Article 173-4 of the Code of Ukraine on Administrative Offenses, as amended by this law, the state bears responsibility for responding to incidents of bullying involving minors – whether as victims or perpetrators – particularly when such actions result in psychological or physical harm. More broadly, bullying is defined as behavior that encompasses psychological, physical, economic, or sexual violence, including acts committed through electronic means of communication.

Regarding adults, although current Ukrainian legislation does not explicitly address online bullying beyond the contexts of secondary education and employment, this does not equate to an absence of legal protection. Certain groups, however, are afforded specific legal safeguards. For instance, journalists receive enhanced protection against cyberbullying. Specifically, Part 2 of Article 171 of the Criminal Code of Ukraine provides that any attempt to influence a journalist with the intent to hinder their professional activities or to persecute them constitutes a criminal offense punishable by fines, arrest, or restriction of liberty.

While the legislation does not explicitly delineate the methods or means by which such influence may be exerted, interference through electronic communications, including cyberbullying, can be encompassed within the scope of this provision. Consequently, any actions aimed at undermining a journalist’s professional duties via digital platforms may be recognized as a criminal offense under Article 171 of the Criminal Code of Ukraine.

In cases where online bullying is motivated by ethnic, racial, or similar factors, such acts of cyberbullying may constitute a criminal offense under Article 161 of the Criminal Code of Ukraine, titled “*Violation of Equality of Citizens*.” This provision criminalizes intentional actions aimed at inciting hostility or hatred based on nationality, race, or religious beliefs; degrading national honor and dignity; offending citizens’ religious sentiments; or engaging in conduct that restricts rights or grants privileges based on race, skin color, political or religious views, gender, disability, ethnic or social origin, property status, place of residence, language, or other similar criteria. The penalties for such offenses include fines, imprisonment for up to five years, or imprisonment for up to three years with the potential deprivation of the right to hold certain positions or engage in specified activities.

It is essential to emphasize that, for actions to qualify under this article, they must not only formally correspond to the listed characteristics (or related criteria through genetic, functional, or systemic associations), but must also result in significant harm to protected social relations. In other words, the conduct must be of a socially dangerous nature to warrant criminal liability under Article 161.

In the most severe cases where cyberbullying results in suicide or attempted suicide, the perpetrator may be held criminally liable under Article 120 of the Criminal Code of Ukraine. According to the Resolution of the Plenary Session of the Supreme Court of Ukraine dated February 7, 2003, No. 2, which addresses judicial practice in cases concerning the protection of human life and health, Part 1 of Article 120 establishes liability for driving an individual to suicide through cruel treatment, blackmail, coercion to commit unlawful acts, or systematic humiliation of dignity. Here, cruel treatment encompasses actions that inflict physical or psychological suffering, whereas systematic humiliation involves prolonged insults or mockery directed at the victim’s dignity. Nonetheless, legal scholarship observes that the judicial application of Article 120 remains limited and is documented in only a small number of individual cases.

Civil law protection against cyberbullying in Ukraine is multifaceted and encompasses several critical aspects. Primarily, victims of cyberbullying are entitled to seek the retraction of false information disseminated about them online. This right enables individuals to petition the court to remove defamatory content or to demand a public retraction where their rights and reputation have been infringed.



Secondly, victims of cyberbullying are entitled to exercise their *right to reply* in response to evaluative judgments. This right allows individuals to formally address accusations or comments that cause distress, thereby providing an opportunity to rebut false information or correct distorted facts.

Moreover, a fundamental aspect of civil law protection involves claims for compensation for both moral and material damages. Victims may initiate legal proceedings to obtain redress for the emotional suffering caused by defamatory statements or insults. Additionally, they may seek compensation for material losses incurred as a direct consequence of cyberbullying.

It is important to emphasize, however, that the effectiveness of these remedies depends largely on the ability to identify the perpetrators. In the digital environment, this poses a considerable challenge due to the anonymity afforded to users and the difficulties inherent in tracing the source of harmful content.

Furthermore, internal regulations and policies enforced by website administrators and social media platforms play a vital role in combating cyberbullying. These platforms are obligated to establish and implement measures aimed at preventing the dissemination of hateful content and harassment. The jurisprudence of the European Court of Human Rights, particularly in landmark cases against Estonia and Norway, has established a precedent affirming the responsibility of platform owners for failing to adequately address offensive content and for insufficient content moderation practices that may facilitate systemic bullying.

Thus, civil law offers a comprehensive set of mechanisms to address cyberbullying. However, the effectiveness of these protections largely depends on the ability to identify those responsible for such violations, as well as on the active cooperation of online platform administrators in enforcing relevant policies.

A closely related phenomenon that intersects with both cyber hygiene and online abuse is hate speech. Although there is no universally accepted legal definition of hate speech, the concept is addressed in international legal instruments and non-binding soft law frameworks. One of the most widely cited definitions is provided in the Recommendation of the Committee of Ministers of the Council of Europe.

According to Recommendation R (97) 20, hate speech is defined as “any form of expression that promotes, incites, encourages, or justifies racial hatred, xenophobia, anti-Semitism, or other forms of intolerance, including intolerance expressed in the form of aggressive nationalism and ethnocentrism, discrimination, and hostility against minorities, migrants, and people of immigrant origin.”

This definition highlights several key dimensions of hate speech, each of which carries distinct legal implications and challenges for its regulation and the protection of affected individuals.

The first defining characteristic of hate speech is its expression that “promotes, incites, encourages, or justifies racial hatred, xenophobia, anti-Semitism, or other forms of hatred.” This implies that hate speech is not limited to overtly hostile or aggressive statements; rather, it also encompasses language that may appear subtle or indirect but serves to cultivate a culture of intolerance or to legitimize discrimination against specific groups.

The second element of the definition emphasizes “intolerance, including intolerance expressed in the form of aggressive nationalism and ethnocentrism.” This indicates that hate speech can be disguised as a defense of national interests or the preservation of traditional values, while in practice functioning to marginalize, stigmatize, or demoralize other social groups.

The practical application of these characteristics presents several challenges. First, identifying hate speech often requires a nuanced understanding of the context in which a statement is made. It can be difficult to determine whether language “promotes or justifies” hatred, particularly when such rhetoric is embedded in discussions of politics, national security, or cultural identity.

Second, the broad spectrum of hatred covered by the definition—including xenophobia, anti-Semitism, and other forms of intolerance—necessitates a multidimensional approach to both analysis and enforcement. While this complexity complicates the operationalization of the definition, it also

enhances its capacity to address the varied and evolving manifestations of hate in contemporary discourse.

Mostly, while the application of the definition of hate speech requires careful consideration and thorough contextual analysis, it remains an essential tool in the fight against discrimination and in the promotion of tolerance and mutual understanding within society. Its significance lies in its broad scope, which encompasses not only direct expressions of hatred but also statements that incite, legitimize, or justify intolerance and discrimination, and is based on various personal or group characteristics. This concept has played a critical role in shaping legislative and policy frameworks in numerous countries and continues to inform international human rights discourse and initiatives.

Within fields such as social sciences, law, and cyberpsychology, hate speech is understood as any form of expression that incites, endorses, or legitimizes hatred, discrimination, or hostility toward individuals or groups on the basis of characteristics such as race, ethnicity, nationality, religion, gender, identity, age, or disability.

Within the context of cyber hygiene—an increasingly important dimension of digital culture that encompasses practices aimed at ensuring a safe and respectful online environment—hate speech represents a significant threat. It contributes to the creation and reinforcement of toxic digital spaces, thereby undermining initiatives designed to foster secure, inclusive, and civil online communication.

Hate speech in the online environment not only threatens individual well-being but also undermines the social fabric by fostering division, prejudice, and hostility within communities. Its psychological impact, particularly vulnerable groups such as youth and minorities, can be profound and long-lasting, manifesting in outcomes ranging from anxiety to severe mental health disorders. In an era where digital communication is both instantaneous and far-reaching, the imperative to address hate speech has become increasingly urgent.

The concept of cyber hygiene is critical in mitigating the harmful effects of hate speech; however, its effective implementation requires coordinated engagement from all stakeholders, including individuals, communities, and digital platform administrators. Online platforms must adopt proactive strategies, including the development and enforcement of robust mechanisms to detect and filter harmful content, while simultaneously fostering ethical and responsible digital behavior. Equally important is the integration of digital ethics education and the cultivation of critical thinking skills, which empower users to identify, challenge, and respond appropriately to hate speech.

Technological advancements in artificial intelligence (AI) and machine learning offer substantial potential for addressing hate speech at scale. These tools can enable the swift and efficient identification of harmful content. However, they also raise critical concerns regarding the balance between necessary content moderation and the preservation of freedom expression. These concerns extend beyond theoretical debates and have tangible implications for policy-making and the future architecture of digital communication.

Accordingly, the challenge of countering hate speech in the digital sphere demands a balanced, multidimensional approach that integrates legal mechanisms, technological innovations, and a sustained societal commitment to advancing digital literacy and accountability. By cultivating an online environment grounded in respect, empathy, and mutual understanding, it becomes possible not only to protect individual well-being but also to uphold the integrity and inclusivity of the digital space.

## 5. Conclusions.

As cyber threats are constantly growing in sophistication and scale, legal instruments must serve as a fundamental line of defense, ensuring the protection of digital rights and freedoms. In this context, the law remains an indispensable mechanism for combating cybercrime and upholding the integrity of the digital environment.

Given the dynamic and increasingly complex nature of cybercrime, legislative measures must be subject to continuous review and adaptation to effectively counter emerging threats. Particularly

insidious manifestations of digital harm, such as cyberbullying and hate speech, may cause long-term psychological damage, disproportionately affecting vulnerable groups. Addressing these challenges necessitates not only the establishment of comprehensive legal provisions but also the effective identification of perpetrators and the prompt, coordinated action of law enforcement agencies and digital platform administrators.

The responsibility of technology platforms in moderating harmful content is particularly crucial. A failure to respond effectively to abusive or unlawful behavior not only risks legitimizing such actions but also contributes to the emergence of a culture of impunity.

Therefore, a comprehensive, multifaceted approach, encompassing legal, technological, and institutional measures, is essential to mitigate the risks associated with poor cyber hygiene and to promote a safer, more accountable digital environment.

Furthermore, legal frameworks are insufficient to fully mitigate the challenges associated with cyber hygiene. A truly holistic approach requires sustained efforts in user education and awareness. Enhancing digital literacy, promoting responsible online behavior, and increasing awareness of emerging cyber threats are foundational elements in fostering a safer and more resilient digital environment. It is imperative to foster a digital culture characterized by respect, accountability, and critical thinking. Only through sustained investment in education can society hope to preempt the most deleterious consequences of cyber threats.

As technological innovation advances at an unprecedented pace, legal and regulatory systems must remain agile, adaptive, and forward-looking. This involves not only addressing established forms of cybercrime but also anticipating novel risks arising from emerging technologies such as artificial intelligence and deep learning. Additionally, the protection of privacy and data security must remain a central priority, given the growing entwinement of digital technologies with personal, professional, and social spheres.

Finally, ensuring cybersecurity in the digital age requires a comprehensive, multidimensional strategy that integrates legal frameworks, technological innovation, and educational initiatives. By adopting such an approach, it is possible to preserve the digital sphere as a space for opportunity and innovation while minimizing its inherent risks to individuals and society at large.

## References:

1. Biliavska, Yu.V., & Shestak, Ya.I. (2022). Cybersecurity and cyber hygiene: The new era of digital technologies. *International Scientific and Practical Journal "Goods and Markets"*, 3-2022, p. 47-59.
2. Drishliuk, V.I. (2005). Regarding the definition of the concept of "abuse of civil rights". *Actual Problems of State and Law*, 25, p. 242-246.
3. Klymchuk, O.O. (2013). Legal bases of cyber security in Great Britain. *Information Security: Challenges and Threats of Modern world*, p. 87-90.
4. Kozubtsov, I.M., Sameliuk, V.P., & Yavych, M.P. (2023). Review of the definition of cyber hygiene in scientific literature and public opinions. *Proceedings of the IX International Scientific and Practical Conference on Problems of Higher Education and Science "Information Technologies in Education, Science and Production (ITONV-2023)"*, May 25-26, 2023. Lutsk: Image and Promotion Department of LNTU, p. 301-304.
5. Sverdlyk, Z. (2022). Cybersecurity and cyber protection: Agenda issues in Ukrainian society. *Ukrainian Journal of Library and Information Sciences*, 10, 175-188 [in Ukrainian].
6. Sopilko, I.M. (2021). Features of countering cyber threats by legal methods and means. *Legal Bulletin*, 4(61), p. 105-110.
7. Subotka, V., & Medvedenko, N.V. (2022). Legal regulation and subjects of cyber security in Ukraine. *Cybersecurity in Ukraine: Legal and Organizational Issues: Materials of the International Scientific and Practical Conference*, Odessa, November 23, 2022. Odessa: ODUVS, p. 19-22.



8. Tishchenko, V.O., & Lohvynenko, Ye.S. (2023). Legal principles of ensuring cybersecurity in conditions of martial law. *Counteraction to Cybercrime and Trafficking in Human Beings: Collection of Materials of the International Scientific and Practical Conference*, Vinnytsia, May 31, 2023. Vinnytsia: KHNUVS, p. 71-73.
9. Shagaka, O. V. (2021). Compensation for damages caused as a result of abuse of rights in online contracts. *Doctoral Thesis in Law*, Odessa, p. 180.
10. Council of Europe. (1997). Recommendation No. R (97) 20 on "hate speech" and its Explanatory Memorandum. Retrieved from [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=0900001680505d5b](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680505d5b).

---

**Svitlana Petrenko,**  
Researcher, Scientific and Organizational Center  
National Academy of the Security Service of Ukraine  
E-mail: [sveta.iris.av@gmail.com](mailto:sveta.iris.av@gmail.com)  
ORCID: 0000-0003-1219-2401