

# Cybercrime as a Discourse of Interpretations: the Semantics of Speech Silence vs Psychological Motivation for Actual Trouble

**Vitaliy Matveev<sup>†</sup>**

Doctor of Science in Philosophy, Associate Professor at the Department of the Applied Psychology, Institute of Human Sciences, Borys Grinchenko Kyiv University

**Nykytchenko Olena Eduardivna<sup>††</sup>**

Current Position: Associate Professor - Department of Cultural Studies, Art History and Philosophy of Culture - State University «Odessa Polytechnic»

**Nataliia Stefanova<sup>†††</sup>**

Professor Morokhovsky Department of English Philology, Translation and Philosophy of Language, Faculty of Germanic Philology, Kyiv National Linguistic University, Ukraine

**Svitlana Khrypko<sup>††††</sup>**

[s.khrypko@kubg.edu.ua](mailto:s.khrypko@kubg.edu.ua)

Department of Philosophy, Faculty of History and Philosophy, Borys Grinchenko Kyiv University, Ukraine

**Alla Ishchuk<sup>†††††</sup>**

Department of English Philology, Faculty of Foreign Philology, Dragomanov National Pedagogical University, Ukraine

**Katerina PASKO<sup>††††††</sup>**

Associate Professor of the Department of Psychology Educational-Scientific Institute of Pedagogy and Psychology of Sumy State Pedagogical University named after A.S. Makarenko

## Summary

The article studies the discourse and a legal uncertainty of the popular and generally understandable concept of cybercrime. The authors reveal the doctrinal approaches to the definition of cybercrime, cyberspace, computer crime. The analysis of international legal acts and legislation of Ukraine in fighting cybercrime is carried out. The conclusion is made about the need to improve national legislation and establish international cooperation to develop the tools for countering cybercrime and minimizing its negative outcomes. The phenomenon of nicknames is studied as a semantic source, which potentially generates a number of threats and troubles – the crisis of traditional anthroponymic culture, identity crisis, hidden sociality, and indefinite institutionalization, incognito style, a range of manifestations of loneliness – from voluntary solitude to traumatic isolation and forced detachment. The core idea is that it is the phenomenon of incognito and hidden name (nickname and other

alternatives) that is the motivational stimulus for the fact of information trouble or crime.

## Key words:

*Cybercrime, netcrime, loneliness, interpretation contexts, nickname, anthroponyms, values, axioconceptsphere.*

## 1. Introduction

Crime has been inherent in any period, any state, any social formation. But in the postmodern world, a new type of information crime has become particularly relevant – in everyday life and in scientific and legal circles it got the name of cybercrime or netcrime.

Cybercrime is not a traditional crime, but a relatively young phenomenon associated with the birth and spread of the Internet as a postmodern happening. Due to its antisociality and hidden identity (the latter is provided by the nickname), this type of crime from the very beginning proved to be more than just convenient and easy for intruders, scammers, offenders, and mere network hooligans. In addition to the informational and psychological imbalance, which usually

become the logical result of cyber violations, it makes sense to mainstream the economic benefits of such actions. After all, especially often such crimes in the space of network culture are committed with a pragmatic motive of illicit enrichment.

The unique nature of cybercrime is revealed in the dualism of speech silence and real offense. After all, the peculiar nature of the World Wide Web has provided global users with anonymity, which has undoubtedly become a potential determinant of this type of crime. The dissonance of visualization of this phenomenon determined the purpose of the study and the authors' interest in the idea of cybercrime as a discourse of interpretations.

*The analytical discourse* of the general problem is presented in the works and research of such scholars as J. Aras, O. Baev, R. Beliakov, J. Bloombecker, V. Markov, M. Ozhevan, Yu. Onishchenko, O. Orlov, A. Protasevich, P. Pushkarenko, K. Rudoi, Ye. Skulish, V. Khakhanovsky, V. Chernei, and others. I. Diorditsa, D. Dubov, O. Manzhai, Yu. Onishchenko, O. Orlov, P. Pushkarenko, and others have devoted their research to the issue of legal regulation of cybersecurity and countering cybercrime.

*The regulatory framework* of our study is the Constitution of Ukraine, the Criminal Code of Ukraine, the Criminal Procedure Code of Ukraine, the Civil Code of Ukraine, The Economic Code of Ukraine; international documents, namely the Convention on Cybercrime; laws and resolutions of the Verkhovna Rada of Ukraine (the Parliament), acts of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine; decisions of the Constitutional Court of Ukraine, decisions of courts of general jurisdiction, decisions of the European Court of Human Rights, which relate to the fight against organized cybercrime, legislation of foreign countries in terms of protecting their cyberspace.

## 2. Methodology

To ensure the objectivity, comprehensiveness, and completeness of our research as well as obtain scientifically substantiated and reliable results, a set of philosophical and ideological, general scientific, and special methods of scientific knowledge have been used, among which are synthesis, logic, analysis, and generalization of references. We have also used such general scientific methods as historical, comparative, and systematic methods. The historical method allowed studying the features of the formation of providing legal bases for combating organized cybercrime in the economic sphere. Using the comparative method, we compared the provisions of the current legislation of Ukraine, European countries, and international norms on the problems of ensuring the fight against organized cybercrime in the economic sphere. The system method was used to justify the independence of the

principles of creating a system for combating organized cybercrime in the economic sphere. It also enabled us to conceptually form and substantiate the theoretical foundations and develop a framework of categories and concepts. The structured system approach was used to study the problems of legal regulation to solve the issues of implementing and ensuring the fight against organized cybercrime in the economic sphere. Finally, semantic analysis and methods of speech methodology allowed us to reveal the phenomenon of a nickname as a potential threat from the sphere of personal space to the state sphere of humanitarian security.

## 3. Results and Discussion

### 3.1 Ukrainian context of the study

Countering any negative impact requires an understanding of the essence of the problem and knowledge of its genesis. Since the speed of development of society is linked with the achievements of scientific and technological progress and criminal manifestations, it is also important to address the issue of the historical development of the introduction of legal mechanisms to oppose cybercrime abroad and in Ukraine.

The increase of cyber threats to the economic, informational, and political areas of the country makes the issue of optimizing the legal regulation of this area more and more relevant. Besides, under modern conditions, it is important to be ready to accept the necessary changes that will meet European and global standards.

The continuous development of legal regulation of the fight against organized cybercrime in the information and economic sphere of Ukraine is vital. Firstly, today almost all state and non-state economic processes operate via cyberspace tools. Secondly, under conditions of the undeclared war, in which Ukraine is forced to take part, virtual space is one of those fronts at which our country shows poor results, while cyber threats to the national economy take much-needed resources. Thirdly, the level of awareness of the threat of cybercrimes and their danger is still low in society, whereas the subject of a criminal attack is much more complex and incomprehensible to the majority in the community.

Under such conditions, the problem of prospects for the legal regulation of the fight against cybercrime in Ukraine is one of the priorities for research to ensure appropriate changes implemented in practice.

### 3.2 Cybercrime in the genesis of the legal framework and discourse of doctrinal interpretations

The postmodern world broke out with the rapid development and popularization of network culture. The

introduction and development of information and telecommunication technologies logically modeled a new type of Internet culture and potentially contributed to the formation of a cybernetic space. The latter, while influencing the political and socio-economic situation, updates the need to ensure cybersecurity, because today cybercrime poses the greatest threat both to each country individually and entire international community. Thus, the Cybersecurity Strategy of Ukraine states the advantages of the modern digital world and the development of information technologies have led to new threats to national and international security. Along with incidents of natural (unintentional) origin, the number and power of cyberattacks motivated by the interests of particular countries, groups, and individuals are growing [4]. For the successful fight against cybercrime as a dynamic, destructive, and inherently anti-social phenomenon, it is essential to improve the principles of legal regulation of the fight in this area and a clear analytical discourse on related issues.

In Ukraine, the problem of combating cybercrime is complicated by the fact that the term cybercrime is not defined in official regulatory documents (even though the concept is familiar both for the lexicon of law enforcement agencies of Ukraine and countries worldwide, and for the legal doctrine of our state). That is why the degree of threat posed by computer crimes is not fully realized in society due to insufficient scientific development of the fundamental concepts associated with it.

“As new tools and techniques are emerging everyday to make information accessible over the Internet, so is their vulnerabilities” [12]. The Internet is a haven for criminals who, staying anonymous and using the vastness of the network, carry out illegal activities. Any terms with the prefix cyber- have not yet received a well-formed definition either at the scientific or regulatory levels and remain the subject of scientific discussion. The concept of cybercrime is no exception – it is not disclosed even by the norms of the Budapest Convention on Cybercrime of 23.11.2001 [4]. This international document contains guidance on:

- 1) violations against the confidentiality, integrity, and availability of computer data and systems;
- 2) computer-related offenses,
- 3) offenses related to the violation of copyright and related rights. [13]

We can conclude that cybercrime at the international level is understood as a total of these crimes.

### 3.3 Analysis Approach

In Ukraine, cybercrime is primarily associated with virtual space. The issues related to cybercrime are studied by scholars in very different aspects.

The history of the emergence and the specifics of the genesis of cybercrime itself is studied by S. Buiagi [7] in his

dissertation “Legal regulation of the fight against cybercrime: a theoretical and legal aspect”.

As a result of the analysis of the legal doctrine, S. Buiagi identifies four stages in the development of the phenomenon of cybercrime.

- (i) The first stage is preparatory. It covers the period between the late 1960s and early 1970s, which is the initial moment of committing crimes using electronic computers.
- (ii) The second stage – the spread of cybercrime – covers the period between the early 1970s and 1986. This stage marked the emergence of hackers and their organized groups. It ended with the adoption of the first-ever regulatory act on cybercrime and the first-ever arrest of a hacker.
- (iii) The third stage is the period of transnational cybercrime and cyberterrorism (1994 – early XXI century).
- (iv) The fourth stage – the modern stage of cybercrime (XXI century) – the emergence of new forms of computer crimes.

We support the author’s conclusion that the genesis of the development of cybercrime and the genesis of legal regulation of the fight against cybercrime cannot be conflated. Cybercrime is developing as consistent with the evolution of the latest technologies. Therefore, today it is an area that is constantly one step ahead of its regulatory affairs [7]. E. Kovalenko and A. Pletnev support this opinion too. Claiming that cybercrime has a very high potential for developing and increasing its adverse effects, they note the discrepancy between the pace of development of the means of criminal activity in cyberspace and the pace of legislative regulation and the implementation of certain means of countering such activities. [18].

D. Bilenchuk, regarding the interpretation of the phenomenon, declares that cybercrime is a crime in a computer-modeled information space, which contains information about persons, objects, facts, events, phenomena, and processes presented in mathematical, symbolic, or any other form on local and global computer networks. It may also contain information stored in any physical or virtual device, as well as other data storage item specially designed for data storage, processing, and transmission. [6]. O. Ivanchenko similarly understands cybercrime as a set of crimes committed in virtual space with the help of computer systems, computer networks, or other means of virtual space, within computer networks, and against computer systems, computer networks, and computer data. [8]. Therefore, it makes sense to interpret cybercrime as a set of acts, defined by criminal law, which are committed in a particular territory or about objects located on it for the corresponding period, in virtual space by destructive influence on computer systems, computer networks, and computer data.

### 3.4 Legal specifics of the problem

The legal grounds for fighting and opposing cyberterrorism can be divided into two corresponding interrelated levels:

1. International legal acts signed and ratified by Ukraine.
2. National legislation of Ukraine.

International legal acts regulating the fight against cybercrime include the Budapest Convention on Cybercrime of 23.11.2001, which was ratified by the Ukrainian Parliament on 07.09.2005. It is the only legally binding international cybersecurity document that establishes a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international cooperation. The Convention does not define cybercrime although its preamble states that the Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation [9].

To implement the Budapest Convention on Cybercrime of the Council of Europe, the Decree of the President of Ukraine of 15.03.2016 approved the Cybersecurity Strategy of Ukraine. It aims at creating conditions for the safe functioning of cyberspace, its use in the interests of the individual, society, and the country. To achieve this goal, the Strategy provides for the following activities:

- (i) creation of a national cybersecurity system;
- (ii) strengthening the capabilities of security and defense sector entities to ensure an effective fight against military cyber threats, cyber espionage, cyberterrorism, and cybercrime, and deepening international cooperation in this area;
- (iii) providing cyber protection of state electronic information resources, information that is required to protect by law, as well as information infrastructure that is under the Law of Ukraine. The violation of its sustainable functioning will adversely affect the national security and defense of Ukraine (critical information infrastructure).

In general, the cybersecurity strategy of Ukraine defines priority areas for ensuring the cybersecurity of Ukraine, among which the focus is on creating a national regulatory and terminological base in this area, harmonizing regulatory documents in the field of electronic communications, information protection, information- and cybersecurity according to international standards and standards of the EU and NATO. The Strategy has become a source for developing cybersecurity regulations. Another step towards

the legal regulation of cybercrime was the adoption of special law – in 2017, the Law of Ukraine “On basic principles of ensuring the cybersecurity of Ukraine” was adopted [19]. The law defines the legal and organizational basis for ensuring the protection of vital interests of a person and citizen, society and the country, the national interests of Ukraine in cyberspace, the main goals, directions, and principles of state policy in cybersecurity. A lot depend on building systems that can identify and prevent cybercrime. However, “desired features for the cyber attack detection system depend on both the methodology and the modeling approach used in building the cyber attack detection system” [23].

So now, legislatively, such concepts as cybersecurity, cyber threat, cybercrime, cyberspace, etc. are defined. According to the law, cybersecurity is defined as the protection of vital interests of a person and citizen, society, and the country during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace.

Cyberspace is defined as an environment (virtual space) that provides opportunities for communication and/or the implementation of public relations, formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications through the Internet and/or other global data transmission networks.

Defining the concept of cybercrime, the legislator identifies it with the concept of computer crime, noting that cybercrime (computer crime) is a socially dangerous guilty act in cyberspace and/or with its use, the liability for which is required by the Law of Ukraine on Criminal Liability and/or recognized as a crime by international treaties of Ukraine.

Although, this definition is not indisputable. Approaches to determining the correlation of these categories are different both among scientists and in the dictionaries.

According to V. Butuzov, computer crimes and cybercrime are different types of crimes in the field of advanced information technologies. These crimes are classified according to the following criteria:

- (i) crimes are classified as computer crimes due to the tool of committing the crime – computer equipment. V. Butuzov notes that the object of encroachment is public relations regarding automated information processing;
- (ii) crimes are classified as cybercrime due to a specific environment for committing crimes – cyberspace (the environment of computer systems and networks). At the same time, V. Butuzov refers to the list of illegal acts provided for in the Convention and its Additional Protocol. The researcher believes only acts from this list can be classified as cybercrime [2].

Yu. Belsky notes that cybercrime is a crime committed in the process of automated information processed via computers or computer systems. The object of encroachment is public relations in electronic information circulation and other public relations, in which the computer acts as a qualifying sign of committing a crime (for example, computer fraud or cyberterrorism) [5].

O. Kopatin and Ye. Skulishin define cybercrime as a crime related to the use of cybernetic computer systems and a crime in cyberspace. Unlike computer crime, the concept of which is associated with the use of any computer equipment, cybercrime is a narrower concept associated with the functioning of cybernetic computer systems [17].

I. Diorditsa notes that the term cybercrime is often used along with the term computer crime, and often these concepts are used as synonyms. The scholar agrees that these terms are very close to each other, yet he does not consider them synonymous while noting that the concept of cybercrime is broader than computer crime and more accurately reflects the nature of such a phenomenon as a crime in the information space. He supports his point of view with the definitions of the Oxford Dictionary, which defines the prefix “cyber-” as a component of a complex word. Its meaning is related to information technologies, the Internet, and virtual reality [10].

But A. Muzyka and D. Azarov define the identity of the concepts of “cybercrime” and “crimes in the field of computer information”. The researchers note it is necessary to define cybercrime as a crime in the field of computer information [22].

L. Soroka also adheres to the definition of a computer crime as a crime in which the computer is directly the subject and (or) instrument of committing offenses in public spheres related to the use of computer equipment [24].

Summing up, we see that the analysis of doctrinal approaches shows no consensus among scientists in the definition of cybercrime. It is caused by different interpretations of cyberspace and ways of using computer systems in committing illegal actions. Despite the differences, the scholars raise the question of the correlation between international legislation and the legislation of Ukraine regarding the list of illegal actions that are classified as crimes committed in the cybersphere.

So, cybercrime is a relatively new type of socially dangerous act. Conventionally, cyber violations are divided into four groups. The first group includes offenses against the confidentiality, integrity, and availability of computer data and systems. The second group comprises computer-related offenses. The third group consists of crimes related to content. The fourth group covers violations of copyright and related rights.

We state that the main criterion for determining this term is the level of public danger that characterizes the act done. The social context brings us to the factor of social motives

of cybercrime, in general. The motive is in the a priori mixing of the person committing the offense.

Incognito, the ability to act behind the scenes, hidden identity and invisible institutionalization, and other similar factors lead us to the need for more careful consideration of the nickname phenomenon as a psychological motive for the possible crime in the network space.

### 3.5 Nickname as the expression of the crisis in traditional anthroponymy and a factor of multi-contextual hazard

Names are a choice, motivation, wishes, hopes, and a gift from parents. A surname is an inheritance. It is an ancestral sign, a family code, a symbol that connects us with the world of our ancestors, with the history of the family tree. The first name is obtained here and now, and the last name is a voice from eternity, our ancestors' legacy. When one thinks about preserving the family name, handing it down to children, how not to disgrace or lose it, this is the embodiment of philosophy – it is a love of wisdom, a love of knowing your family tree, gratitude to your ancestry [16, 15].

The problem of studying the mystery of history and semantics of names and surnames will never stop being interesting and relevant because it concerns everyone. All people want to know the history of their family, the symbolism of the ancestral surname, etc. As the researchers say, “...anthroponyms are unique linguistic names of the people”, and language, in turn, is “a phenomenon of an ethnic group, people, nation, one of its main features... it is the genetic code of national culture, the key to identity and self-preservation.” [16].

“A name is a creation of language culture; it is a folk phenomenon, which embodies the whole historical layer with all rises and falls; it is, in some sense, a flower that could be real and simultaneously transcendental united with ethnical memory, culture, history, national philosophy and mentality, etc.” [14]. Over time, the names and specifics of their receipt, sound, and purpose change. Our time has created a unique phenomenon of a nickname, which pushes back, minimizes, and, sometimes, destroys the tradition of classical anthroponymy.

The word “nickname” comes from *ekename* that is “additional name”. It is a personal, mostly fictional name that Internet users create to present themselves in various chats, forums, direct messengers but also in Wikipedia, on websites, etc. The English-language lexeme nickname has an Indo-European nature and reaches the root \**auk-* “increase”, “grow”, “gain strength”, semantic transitions of which can be traced in the Old English lexeme *gaeacen* “increased”, “strong”, “capable” [20] and the root \**wak-* “to be cheerful, energetic” with syncretic semantic transitions in the Gothic *wakan* “to observe” and Old English *wacan* “to rise”, “to become alive” [20]. We can assume that the

modern English-language semantic meaning of this lexeme is the result of semantic transitions that function on the designation of a person who, under an assumed name, observes the outside world, communicates, and feels a strong, confident, energetic, and interesting person in this process.

Anthroponyms, first of all, had the function of communication. It should be noted that postmodernism has made significant adjustments here. Electronic communication, which relies on new technologies and provides users with unique opportunities for communication, training, research, and even doing business, is becoming increasingly widespread in our time. The main feature of virtual communication is the relationships of recipients and senders of messages and the roles they take on. Due to anonymity, accessibility, and security, a person creates trust-based relationships with barely known people and even strangers. In virtual reality, such concepts as social status, appearance, age, and gender do not play a big role. The Internet allows you to form a new identity, create a new image and actualize unmet needs. [3]. The rapid development of Internet communication has led to the widespread use of proper names. Almost all information on the Internet is based on the onomastic axis. In Internet communication, the following forms of computer proper name are known for naming users: login, domain name, nickname, chat name, screen name. Whereas the username is usually faceless and represents a number or a simple sequence of letters, the nickname is used for the self-expression of its owner and has a certain semantic load [12]. A nickname, as a means of personalization, implements the intention to attract the interlocutor's attention and mask its true image. As a result, a system of values, or axioconceptosphere, is created, where the meaning-forming motives are INTEREST, the significance of this INTEREST for the individual, and the RESULT that a person predicts to get from the satisfaction of the motivating INTEREST, and which are determined by the biological, social, and individual needs of the individual [25].

### 3.6 Effects of nicknames popularization

The bipolar context of popularizing nicknames and representing virtual communities is exceedingly noticeable. There is a concern that computer information and communication environments (including virtual reality), formed with the help of technical means, over time will increasingly replace ordinary reality, reducing awareness of the "relativity" of inclusion in them. These environments will increasingly influence the formation of a person and his or her identity. Nickname mixes (this is its minimal effect) but rather destroys and breaks the identity as such.

With virtual communities, a unique situation is created in cyberspace that forms a certain subculture, in which many social stereotypes, prejudices, and status-role

conventionalities, which play the role of communication obstacles in real life, lose their meaning. It happens because the Internet user, having only his own nickname, cannot see the interlocutor in cyberspace. It means he cannot know his gender, age, national and racial origin, profession, appearance, or income level. The author of the nickname can make these characteristics public if he chooses to do so. Therefore, priority visualization of the nickname destroys the socialization of the individual.

Virtual culture caused the formation of a new generation of people who identify with other people. It means they simultaneously "co-exist" in two spaces (social and virtual) but prefer to work and relax, communicate, and have fun online. Moreover, we cannot consider these people as the oppressed minorities or groups ignored by society. Virtual culture gradually forms a specific type of person, whose formation and development are largely determined by the system of network interactions.

A particular danger is that virtual culture undoubtedly has a special impact on children and adolescents. They have not yet developed a balanced mentality, and the creation of virtual substitutes and frequent changes in roles can further increase their loss of interest in real life.

Nickname becomes the epitome of third space culture as a threat to national security. Virtual communities are a place where an individual is free from the social barriers that arise as a result of the physical embodiment of identity. However, any member of a virtual community must comply with the rules of this community. Otherwise, he will be "expelled" from it. Yet, at the same time, communities are practically unregulated by the sources external to them and their members; they develop on the principle of self-organizing network spaces. And this is a new type of cultural community of people. These people seem to be united by common interests and regular communication. However, their communication is not set by a rigid framework (although certain mandatory rules exist). So, having their own name in social reality, they get a new name (nickname) in the network, distribute roles in a new way and establish connections that may or may not have an exit from the virtual space to the real one. Virtual communities with all the complex postmodern factors and constants are undoubtedly an attractive phenomenon. It is no coincidence that some virtual communities already number millions of people, but there is also a certain danger. After all, virtuality often becomes a characteristic of a person 1) who gradually loses the ability to self-actualize in society; 2) who loses his freedom instead of access to information and communication environments; 3) who experiences fundamental, deep changes in the gradation of information (mixing vital information with background information, reliable and unreliable, etc.). All these things happen when the socio-cultural space is perceived by the person as a virtual environment saturated with a strong, undivided flow of information of different value. A person loses his identity,

and this is the most dangerous context for popularizing nicknames.

Escape to the virtual world and passion for a nickname (or nicknames) embodies the phenomenon and state of loneliness. Loneliness is the spiritual and ideological “signature” of a person. Just as signature, loneliness can be aesthetically calligraphic, flexible, harmonious and understandable, or vice versa – broken, crossed out, traumatic and painful, impossible to read, perceive and understand [1]. Nickname and everything behind it embodies the state of loneliness that the nickname’s owner experiences – detachment, alienation, voluntary loneliness, conscious solitude, loneliness as a protest, etc. So, nickname is the scar of loneliness that is unique in every person.

Nickname is gradually becoming a universal geopolitical phenomenon that significantly mixes or erases the national flavor of anthroponymic culture. But it should be considered that “geopolitics is inextricably connected with the historical fate of the nation, penetrates its geographical and political parallels” [21]. So, we can assume that the current enthusiasm for nickname-making is a modern cross-section of marginal and assimilative trends in the identity culture, national self-expression, and self-sufficiency.

#### 4. Conclusion

Cybercrime is a set of acts, defined by criminal law, which are committed in a particular territory or in relation to objects located on it for the corresponding period, committed in virtual space by destructive influence on computer systems, computer networks, and computer data. However, the term “cybercrime” is not defined in official regulatory documents, even though the concept is familiar both for the law-enforcement authorities of Ukraine and countries worldwide and for the legal doctrine of our country.

The Internet is and remains the most popular and reliable shelter for a large number of criminals, who, due to their anonymity and the infinity of the network, use it to carry out their illegal activities.

The rapid development of information technology systems will always be ahead of the legislative regulation of relations in this area, including the need to update the list of illegal actions which require criminal liability. It is necessary to improve legislation in this area and bring it in line with international standards. Even though it is undoubtedly appropriate, this is not enough to counter cybercrime. Along with legislative support, fruitful international cooperation should be established to develop mechanisms to counter cybercrime and minimize its negative effects because cybercrime does not depend on borders and the Internet opens unlimited opportunities for criminals from all over the world. Thus, it is necessary to

conduct further scientific developments on countering cybercrime at the national and international levels.

A nickname can be considered a sign that contains a certain worldview, value system, social status, and even ethnocultural stereotypes and represents, from the point of view of cognitive science, a kind of a cast of a new image of self-consciousness. In the process of secondary nomination, nicknames receive emotional-value, emotional-evaluative, and figurative components.

#### References

- [1] Aleksandrova, O., Khrypko, S., Iatsenko, G. Solitude as a Problem of Human’s Mature Choice. *Beytulhikme. An International Journal of Philosophy*, 10 (3), pp. 771–786, 2020. Doi: 10.18491/beytulhikme.1582
- [2] Amelin, O. Definition of cybercrime in national legislation. *Scientific journal of the National Academy of Prosecutor’s Office of Ukraine*, vol. 3, pp. 1–9, 2016 (in Ukrainian). <http://www.chasopysnapu.gp.gov.ua/ua/pdf/11-2016/amelin.pdf>
- [3] Avramova, A. Linguistic features of electronic communication (based on the material of French, English and Russian languages): abstract. for the degree of Candidate of Philology: 10.02.04 “Germanic languages”. Moscow. 2005 (in Russian). <https://www.dissercat.com/content/lingvisticheskie-osobennosti-elektronnogo-obshcheniya-na-materiale-frantsuzskogo-angliiskogo>
- [4] Bieliakov, R. Interaction between the department on combating cybercrime of the Ministry of Internal Affairs of Ukraine with other law enforcement agencies: issues of today. *Law and Security: scientific journal of Kharkiv National University of Internal Affairs*, 4 (55), pp. 85–88. 2018 (in Ukrainian). [http://nbuv.gov.ua/UJRN/Pib\\_2014\\_4\\_18](http://nbuv.gov.ua/UJRN/Pib_2014_4_18)
- [5] Belsky, Yu. On the definition of the concept of cybercrime. *Legal Bulletin*, vol. 6, pp. 414–418, 2014 (in Ukrainian). [http://nbuv.gov.ua/UJRN/urid\\_2014\\_6\\_71](http://nbuv.gov.ua/UJRN/urid_2014_6_71)
- [6] Boichenko, O. Information security in the law enforcement agencies of Ukraine (organizational and legal matters). Manuscript. Crimea. 2009 (in Ukrainian).
- [7] Buyagi S.A. Legal regulation of the fight against cybercrime: the theoretical and legal aspect. Author’s abstract of the thesis for a Candidate of Juridical Sciences: 12.00.01. Kyiv. 2018.
- [8] Buryachok, V., Tolubko, V., et al. Information and cybersecurity: a sociotechnical aspect. Textbook. Kyiv. 2015 (in Ukrainian). <https://law.sspu.edu.ua/files/documents/books/library/3/buryachok.pdf>
- [9] Council of Europe, Convention on Cybercrime, 23 November 2001, available at: <https://www.refworld.org/docid/47dfb202.html>
- [10] Diorditsa, I. The concept and content of cyber threats at the present stage. *Entrepreneurship, economy and law*, vol. 4, pp. 99–107, 2017 (in Ukrainian). [http://nbuv.gov.ua/UJRN/Pgip\\_2017\\_4\\_22](http://nbuv.gov.ua/UJRN/Pgip_2017_4_22)
- [11] Faysel, M. A., Haque, S. S. Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems. *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, No. 7, pp. 316–325. [http://paper.ijcsns.org/07\\_book/201007/20100741.pdf](http://paper.ijcsns.org/07_book/201007/20100741.pdf)

- [12] Galichkina, E. Names of self-presentation in online Internet communication. Debatable issues of modern linguistics. Kaluga. pp. 37–44, 2005 (in Russian).
- [13] Gorova, S. Cyber professionals and cybercrime. Fighting organized crime and corruption (theory and practice), vol. 2 (33), pp. 170–173, 2014 (in Ukrainian). [http://nbuv.gov.ua/UJRN/boz\\_2014\\_2\\_41](http://nbuv.gov.ua/UJRN/boz_2014_2_41)
- [14] Khrypko, S., Iatsenko, G. Philosophy of a Name: Ukrainian Context. Beytulhikme. An International Journal of Philosophy, 9 (2), pp. 437–451, 2019. Doi: 10.18491/beytulhikme.1477
- [15] Khrypko, S., Iatsenko, G. Philosophy of a Surname: Ukrainian Context Beytulhikme. An International of Philosophy, 9 (4), pp. 899–912, 2019. Doi: 10.18491/beytulhikme.1521
- [16] Khrypko, S., Kolinko, M., Iatsenko, G. Philosophical understanding of the semantics of Ukrainian anthroponymy: the phenomenon of surnames. Worldview – Philosophy – Religion, 15, pp. 162–171, 2020 (in Ukrainian). [https://elibrary.kubg.edu.ua/id/eprint/33780/1/Khrypko\\_Sv\\_162-171\\_IFE.pdf](https://elibrary.kubg.edu.ua/id/eprint/33780/1/Khrypko_Sv_162-171_IFE.pdf)
- [17] Kopatin, O., Skulishin, Ye. Dictionary of cybersecurity terms. Kyiv, 2012 (in Ukrainian).
- [18] Kovalenko, Ye., Pletnirov, O. Prerequisites for threats in information security and prospects for overcoming them. Actual problems of Information Security Management in Ukraine: All-Ukrainian Xth Conference (Kyiv, 4 April 2019), pp. 57–61, 2019 (in Ukrainian). [http://ippi.org.ua/sites/default/files/konf\\_04\\_04\\_2019.pdf](http://ippi.org.ua/sites/default/files/konf_04_04_2019.pdf)
- [19] Law of Ukraine “On the basic principles of ensuring cybersecurity in Ukraine”, 5 October 2017. <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- [20] Levitsky, V. Etymological Dictionary of Germanic languages. Vinnytsia: New Book, Vol. 1, 2010.
- [21] Levyk, B., Aleksandrova, O., Khrypko, S., & Iatsenko, G. Geo-policy and Geo-psychology as Cultural Determinants of Ukrainian Religion, Mentality, and National Security. Journal of History Culture and Art Research, 9(3), pp. 217–225, 2020. Doi: 10.7596/taksad.v9i3.2761
- [22] Lisovyi, V. “Computer” crimes: a matter of qualification. Law of Ukraine, vol. 2, 2002 (in Ukrainian). <https://www.crime-research.ru/library/lisovoy.htm>
- [23] Singh, S., Silakari, S. A Survey of Cyber Attack Detection Systems. IJCSNS International Journal of Computer Science and Network Security, vol. 9, No. 5, pp. 1–10. [http://paper.ijcsns.org/07\\_book/200905/20090501.pdf](http://paper.ijcsns.org/07_book/200905/20090501.pdf)
- [24] Soroka, L. Types of offenses in the computer and information technologies. Scientific Journal of Kirovograd State Pedagogical University. Historical Sciences, vol. 9, pp. 262–270, 2005 (in Ukrainian).
- [25] Stefanova, N. Ethnosemiometric parametrisation of axioconceptosphere in the British and Ukrainian linguocultures. Author’s abstract of the thesis for a Doctoral Degree in Philology: 10.02.17., 10.02.21. Kyiv, 2020.



**Vitaliy Matveev**, Doctor of Science in Philosophy, Associate Professor at the Department of the Applied Psychology, Institute of Human Sciences, Borys Grinchenko Kyiv University  
<https://orcid.org/0000-0001-9914-2233>



**Nykytchenko Olena Eduardivna**, Current Position: Associate Professor - Department of Cultural Studies, Art History and Philosophy of Culture - State University «Odessa Polytechnic»  
<https://orcid.org/0000-0002-9403-9795>



**Nataliia Stefanova**, Doctor of Science in Philology, Associate Professor, Professor at Professor Morokhovskiy Department of English Philology, Translation and Philosophy of Language, Faculty of Germanic Philology, Kyiv National Linguistic University (Ukraine). Her scientific interests include comparative-historical and typical linguistics, psycholinguistics, linguoculturology, cognitive linguistics, axiolinguistics. <https://orcid.org/0000-0002-8699-9219>



**Svitlana Khrypko** received the B. E., M. E., and Cand. of Philosophy degrees. She has been an Associate Professor at Department of Philosophy, Faculty of History and Philosophy, Borys Grinchenko Kyiv University since 2018. Her research interest includes axiology, culturological studies, ethnic studies, philosophy of education, multiculturalism of virtual communities.  
<https://orcid.org/0000-0001-9426-4549>





**Alla Ishchuk,**

M. A. (Philology), Ph.D. (Philosophy), Associate Professor at the Department of English Philology, Faculty of Foreign Philology, Dragomanov National Pedagogical University (Kyiv, Ukraine). Her research interests include semantics, Business English, psycholinguistics, philosophy of education.

<https://orcid.org/0000-0001-7825-4295>

**Katerina PASKO** (Candidate of Philosophical Sciences) is the Associate Professor of the Department of Psychology Educational-Scientific Institute of Pedagogy and Psychology of Sumy State Pedagogical University named after A.S. Makarenko. ORCID iD: <https://orcid.org/0000-0003-0488-9719>