Cybercrime in the Economic Space: Psychological Motivation and Semantic-Terminological Specifics

Vitaliy Matveev[†]
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[††]

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

Nataliia Stefanova[†††]

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

Svitlana Khrypko[††††]

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

Alla Ishchuk[†††††]

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

Olena Ishchuk[††††††]

Department of General Studies, Ukrainian American Concordia University, Ukraine

Tetiana Bondar[†††††††]
Associate Professor,
Associate Professor of the Department of Philosophy,
Borys Grinchenko Kyiv University,

Abstract
The article reveals the essence of cybercrime, approaches to understanding this concept, classification of cybercrime, and other illegal acts in this area. The concept of cybercrime has multi-discourse nature and a certain legal uncertainty. Cybercrimes, their forms and types are analyzed in the economic context. The research vocabulary of the economic industry is defined. The scope and content of concepts denoted by the terms of the sphere covered by cybercrime are studied, and its types and forms are analyzed. The article studies problems, achievements, and prospects of resisting and combating cybercrime during the development of the civil information society and Ukraine's entry into the global information space. The study focuses on the economic motivation of most cybercrimes since some material benefit from the fact of cyber offenses is assumed directly or indirectly.

Key words:
cybercrime, interpretation contexts, semantics of definitions, research vocabulary, polysemantics of terminological culture.

1. Introduction

The rapid development of information technologies in Ukraine over the past decade is inexorably accompanied by the dynamic development of crimes in this area. As we can conclude from historical experience, any development and progress that gave humanity civilizational benefits and new opportunities have always been accompanied by negative phenomena. In this case, mass computerization and the rapid development of digital technologies, which have significantly simplified human life, are no exception. So, cybercrimes constitute the most dynamic group of socially

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.18

dangerous acts because cybercrimes become more widespread and dangerous every year. "Cybercrime is an inevitable consequence of the globalization of information processes and, as a result, is the main threat of socio-humanitarian components. The growing number of cybercrime activities in enterprises, the continuous advancement of information technologies, and new opportunities for "improving" the tools for their commitment create economic threats to global information networks." [12].

In the era of information technology, it is impossible to feel protected in cyberspace. With the development of technology, the number of crimes in this area is rapidly growing, and therefore it is safe to say that it is cybercrime in the XXI century that will remain among the most numerous offenses. Most modern researchers pay attention to the originality of such offenses and the fundamentally economic component in the motivation of this activity, claiming that "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 … 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." [8].

In Ukraine and around the world, tens of thousands of crimes are committed annually – these crimes are related to the use of information and communication technologies, software, hardware, other technical and technological means and equipment. Every day, people and companies steal personal data, money from their accounts, collect a lot of confidential and commercial information, block their activities, etc. However, the success of preventing such crimes, exposing them, and bringing the perpetrators to justice is still quite rare compared with the number of such offenses. "Cybersecurity is essentially important because intelligent devices are mostly deployed in a hostile environment" [1].

This does not come as unexpected because cyberspace is infinite, and experienced hackers have all the necessary skills and means to remain incognito in it. Today, cyber-attacks harm not only individuals and legal entities but also countries. Every year hundreds of events of various levels are held worldwide to discuss current cybersecurity issues. New terms and their definitions are constantly appearing in dictionaries of the common lexis and terminological ones. "Change in semantics and appearance of semantic neologisms is a significant phenomenon for the evolution and enrichment of vocabulary. Quite often such changes are accompanied by the change of a stylistic marker of the word, in other words–by its stylistic re-focusing" [6]. There was a need to regulate this terminology and even develop a research vocabulary that will define the study's concepts and terms. So, we can define the following words among the neologisms: cyber intelligence, cyberterrorism, cyber espionage, cyberspace, critical infrastructure, etc. Cybersecurity and the fight against cybercrime in the XXI century are among the most important issues that require in-depth analysis, development, and implementation of high-tech solutions in order to prevent and expose cyber threats. "Prevention of the main threats of cybercrime becomes particularly relevant in the context of hybrid war, the use of mass media and of its communication components. According to the research results, the problem of cybercrime concerns not only the country as a whole but also individual economic entities and almost every person." [12]. It is repeatedly claimed that "maintaining data integrity and privacy is a task for which every official in any sector bears responsibility. Information security is not limited to organizations, but to individuals as well." [5].

Every year cybercrime causes a lot of damage to countries and individuals. At the 73rd session of the UN General Assembly, Secretary-General António Guterres estimated the annual damage caused by cybercrime in the world at $1.5 billion. Unfortunately, the forecasts of cybersecurity experts are disappointing. In the future, the number of crimes and losses from cyberattacks will only grow because offenders usually are at least one step ahead of the mechanisms which government authorities and individuals have to prevent and solve such crimes.

"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" [8]. However, we realize that any crime in cyberspace is not just the embodiment of loneliness (or breakdown) or the desire to prank a person or community. This is, first of all, the embodiment of the intention to get any kind of material benefit. So, cybercrime is a psychological motivation for material benefits and enrichment in an illegal way. It is this specificity of cyber fraud that has determined the purpose and content of our research.

2. Methodology

We used a classical set of philosophical and ideological, general scientific methods to implement the problem completeness of our research and obtain scientifically based and reliable results and universally sought conclusions: synthesis, logic and structure of the presentation, analysis and generalization of problem sources.

Linguistic methodology and method of cognition are used to study the problematic issues of this work in the unity of their speech, visual, and actual perception, social content, a legal and terminological form of representation.

The systemic and structural approach was used to substantiate the separateness and independence of the dominants of building a system to ensure the fight against organized cybercrime in the economic sphere. The same method made it possible to conceptually form and realize the theoretical foundations and definitive discourse on key concepts and to model the complexity of the research discourse.

Semantic analysis and methods of speech methodology allowed us to reveal the phenomenon of a variety of hacking terminology as a potential threat in the sphere of private space, state security, and cultural and humanitarian security.

3. Results and Discussion

3.1 Cybersecurity and cybercrime

Ukraine, like all countries of the world, faces daily challenges in cybersecurity. In the last few years, government authorities have been repeatedly attacked from cyberspace. The launch of the Petya malware on 27.06.2017 disrupted the work of Ukrainian state-owned enterprises, institutions, banks, media, etc. As a result of the attack, the activities of such enterprises as Boryspil Airport, Chernobyl Nuclear Power Plant, Ukrtelecom, Ukrposhta, Oschadbank, Ukrzaliznytsia, and many other large enterprises were blocked. The information systems of the Ministry of Infrastructure, the Cabinet of Ministers, the websites of the Lviv City Council, the Kyiv City state administration, the cyber police, and the Special Communications Service of Ukraine were also affected. “That is why the issue of studying and borrowing positive international experience in the area of administrative and legal mechanisms for regulating information protection in modern conditions, countering cybercrime is also relevant for ensuring Ukraine’s strategic intentions regarding European and Euro-Atlantic integration.” [2].

The legal framework does not stand aside from the problems in the online world. That is why Ukraine adopts relevant laws regulating relations in this area on the legislative level. As of the beginning of 2019 the legal basis of cyber security of Ukraine includes the following normative legal acts: the Constitution of Ukraine, the Criminal Code of Ukraine, the laws of Ukraine “On the Basic Principles of Ensuring Cybersecurity of Ukraine”, “On Information”, “On Information Protection in Information and Telecommunications Systems”, “On the Basics of National Security”, the Doctrine of Information Security of Ukraine, the Council of Europe Convention on Cybercrime, and other international treaties, which are agreed by the Parliament of Ukraine.

According to Ukrainian legislation, cybersecurity is the protection of vital interests of a person and citizen, society and the country in the process of using cyberspace that 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 [7]. In a global sense, cybersecurity is the implementation of measures to protect networks, software products, and systems from digital attacks.

Trying to define the phenomenon of cybercrime, we can notice a certain discoursivity and multi-interpretation in definitions and interpretations. The concept of cybercrime first appeared in American and then other resources in the early 1960s and was defined as a violation of other people's rights and interests concerning Automated Data Processing Systems. The concept of cybercrime as a set of crimes applies to all types of crimes committed in the information and telecommunications sphere, with information, information resources, and information technology being the subject (or purpose) of criminal attacks or the environment in which offenses occur, or the means or instrument of crime. Thus, cybercrime can be defined as a set of crimes committed in cyberspace using computer systems or computer networks and other means of accessing cyberspace, within computer systems or networks, against computer systems, computer networks, and computer data [3.]. Kopan and Skulish define the concept of cybercrime as a crime related to the use of cybernetic computer systems and a crime in cyberspace [4]. According to Bolgov, cybercrime is a set of criminal, socially dangerous acts (activity or inactivity), entrenching on the right of protection against unauthorized distribution and use of information, negative consequences of the influence of information, or the functioning of information technologies. Also, this term includes other socially dangerous acts related to the violation of ownership of information and information technologies, the rights of owners or users of information technologies to receive or distribute reliable and complete information on time [2]. The theory lacks a generally accepted legal definition of the concept under study. Thus, at the doctrinal level, you can find a number of similar homogeneous concepts, in particular: crimes committed using computers, computer crime, crime in the area of cutting-edge technologies, communication crime, cybercrime, crime in the area of computer information, network crime, and the like. The researchers often use the concepts of high-tech crime, cyber crime, network crime, which are used to define crimes in the area of cutting-edge technologies, cybercrime, and crimes in computer networks [11]. So, summing up the above, we can say that cybercrime can be considered a unifying concept that characterizes related criminal actions: cyber-dependent and cyber-

forming crimes. Cyber-dependent crimes are crimes committed using computers, computer networks, or other forms of communication (spreading viruses and other malware, hacking, breaking down servers to hijack network infrastructure or web pages). Such crimes are aimed at damaging computers and network sources and have consequences in the form of fraud. A cyber-forming crime is a traditional type of crime that has become cybercrime through the use of computers, computer networks, and other types of communication. Unlike cyber-dependent crimes, they can also be committed without using a "computer element" [9].

According to the Convention on Cybercrime, which has been part of Ukrainian legislation since 11.10.2005, cybercrime is divided into four types:

1) The first type includes offenses against the confidentiality, integrity, and availability of computer data and systems. This type of cybercrime can include all crimes directed against computer systems and data (for example, intentional access to or part of a computer system; intentional damage, destruction, deterioration, modification, or concealment of computer information; intentional commitment, without having the right to do so, of manufacturing, selling, acquiring for use, distributing, or otherwise providing devices, including computer programs).

2) The second type of cybercrime includes offenses related to computers. Such crimes are characterized by an intentional act resulting in the loss of the property of another person through any introduction, modification, destruction, or concealment of computer data or any interference with the functioning of a computer system, with the fraudulent or dishonest purpose of acquiring, without having the right to do so, economic benefits for yourself or another person.

3) The third type of cybercrime covers offenses related to the content, which consists in committing deliberate illegal actions to develop, offer or provide access, distribute child pornography, as well as possession of such files in their system.

4) The fourth type comprises intentional actions related to the violation of copyright and related rights, in accordance with the requirements of the Berne Convention for the Protection of Literary and Artistic Works, the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights, and the WIPO Copyright Treaty, and the national legislation of Ukraine.

It is worth noting that there are other classifications of cybercrime, but the one proposed by the Convention is the most popular and in-demand with the researchers.

In Ukraine, cybersecurity policy is assigned to a number of government authorities, namely the State Service for Special Communication and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine, and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine. Each of these bodies has corresponding divisions.

The main articles of the Criminal Code of Ukraine that investigate cybercrime in Ukraine are as follows: Article 176 "Copyright and related rights violations"; Article 190 "Fraud"; Article 361 "Unauthorized interference in the operation of electronic computers, automated systems, computer networks, or telecommunication networks"; Article 361-1 "Creation for the purpose of using, distributing, or selling malicious software or hardware, and their distribution or sale"; Article 361-2 "Unauthorized sale or distribution of information with restricted access stored in electronic computers, automated systems, computer networks or on the carriers of such information"; Article 362 "Theft, misappropriation, corruption of computer information or taking possession of it by fraud or abuse of official position"; Article 363 "Violation of the rules of operation of automated electronic computing systems"; Article 363-1 "Obstruction of the operation of electronic computers, automated systems, computer networks, or telecommunication networks by mass distribution of telecommunication messages".

The dynamics and vector of cybercrime detection (in the example of Ukraine) can be traced on the Unified State Register of Court Decisions platform. We can find a certain number of court decisions made on the results of criminal proceedings. The Register contains sentences under these articles and decisions of investigating judges on criminal proceedings that are currently being conducted by pre-trial investigation bodies. So, taking into account the information from this Register, we can argue that Ukraine is currently fighting cybercrime.

3.2 Forms and polyvecor nature of hacking

Hackers have many opportunities to exploit cybersecurity vulnerabilities and achieve their criminal goals. It becomes clear that "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" [13]. Today, we can distinguish the following most popular methods, which are represented by the following derived and compound terms. Carding – fraudulent transactions with credit cards (credit card details) that are not approved by the cardholder. This can be theft or illegal receipt of a credit card, copying card data for further forgery, copying card details for making purchases via the Internet without the participation of the cardholder. In any case, the main goal of criminals is to gain access to other people's money. To achieve this goal, attackers come up with a variety of ways to get the necessary information from inattentive and gullible citizens. One of these ways is phishing.

Phishing is a type of Internet fraud that suggests sending messages to the victim on behalf of well–known companies

or organizations (for example, a bank, tax service, or recognizable online store), but, in reality, they are not authentic. The purpose of phishing is to gain access to confidential user data (passwords, logins, personal accounts, and bank card data). Usually, the criminals use a method of conducting mass mailings on behalf of popular companies or organizations that contain links to fake sites that are difficult to distinguish from real ones. In such an email the person is politely asked to update or confirm the correctness of personal information or gets informed about any problems with the data and then redirected to a fake site where the user needs to enter his credentials. If the victim enters his data on such sites, they become revealed to criminals who can use such data for the purpose of stealing personal information, personal finances, or other things. Phishing is one of the most common types of cyberattacks.

Also, there are several types of phishing:

• SMS phishing – a situation when a potential victim of fraudsters receives a message that his credit card has been blocked by the bank, and to unlock it, you need to provide banking details; or the information on a prize "won" by the cardholder, who, however, needs to pay for its delivery. There are many variations of SMS, so a person must be especially careful and attentive to the content of the messages he receives.

• Online phishing – a situation when scammers create phishing (fake) pages that copy the official pages of banks, payment services, online stores, etc. Unfortunately, users do not always carefully check the site name when entering their credit card details, which is in the cyber scammers' interests.

• Vishing is almost the same phishing crime, but attackers use phone calls to lure out card details (scammers often introduce themselves as bank employees and try to find out the PIN from the cardholders or force them to perform some actions with their account).

• Skimming – copying payment card data using a special device (skimmer). It usually occurs when performing card operations with ATMs. Criminals use mini-cameras or replaceable keyboards to get data.

• Shimming – an upgraded type of skimming. In this case, scammers use an almost invisible device that is placed inside the card reader. This way credit card data is copied unnoticed.

• Online fraud – fake online auctions, online stores, websites, and telecommunications facilities.

• Piracy – illegal distribution of intellectual property objects on the Internet.

• Malware - creation and distribution of viruses and malicious software.

• Illegal content - content that promotes extremism, terrorism, drug addiction, pornography, and the cult of cruelty and violence.

• Refiling – illegal substitution of phone traffic.

A virus is software installed without the user's knowledge and against their will on their computer or other devices. A computer virus can be "caught" in different ways. For example, web pages and email attachments can be used to directly launch a virus into the system. The virus is often embedded in a program downloaded from the Internet, which sets a virus free after the "victim" installs it. Once infected with a virus, the program can block access to files and the system for a ransom. However, paying a ransom does not always guarantee that the system will resume working.

Social engineering is an approach to hacking that does not depend on technology. The fraudsters convince the "victim" to disclose confidential information. Tactics can be different: from acting as a bank employee, acquaintance, or friend to various threats demanding to install malware.

Malware – these programs include so-called Trojan, spyware, or adware. They are often installed together with another useful software that the "victim" decided to download. Such programs can secretly record all keystrokes, scan files on your hard drive, and read browser cookies.

Hacking is a deliberate action aimed at unauthorized entry into the software or system by bypassing the security mechanism to obtain unauthorized access to a certain software or system.

And this is not just a list of cybercrime types. It reflects reality. In 2018, the above methods were used in the most high-profile cyber attacks. Last year, hackers broke into T-Mobile servers and stole the personal data of more than 2 million customers. Other hackers (or the same ones) hacked into the Marriott hotel chain's database and stole the data of about 500 million customers. 2017 was marked by the invasion of the WannaCry ransomware, which in May blocked the operation of hundreds of thousands of computers around the world and demanded a transfer of funds for resuming their work. Such cases are not isolated. Thousands of computers, databases, systems, etc. are hacked every day in the world.

That is why there is a need for international coordination of the relevant terminology and semantics of crimes. It should be noted that the vast majority of neologisms are formed by abbreviation – the most active way of word-formation of the XXI century. The essence of the method is to ensure the transmission of the maximum amount of information per unit of time, in other words, to increase the effectiveness of the communicative function of the language. An important factor in the spread of abbreviations in both common lexis and terminology is extralinguistic influence, i.e., socio-economic, political, and cultural conditions. Radical changes in economic life, new directions of economic policy, the introduction of new technologies in various spheres of life, the above–mentioned increase in the flow of information - all these factors contribute to the appearance of neologisms in the language, including abbreviations [14]. Therefore, as part of cooperation in the fight against computer crimes, the INTERPOL working group developed a codifier according

to which all cybercrimes are classified as follows: QA – unauthorized access and interception (QAH – computer boarding (hacking); QAI – interception; QAT – theft of time; QAZ – other types of QA); QD – unauthorized change of computer data (QAD – logic "bomb"; QAD – Trojan horse; AD – computer virus; AD – computer worm; QAD – other kind of QD); QF – computer fraud (QFC – ATM fraud; QFF – computer fake; QFG – fraud with slot machines; QFM – manipulation with the input-output programs; QFP – fraud with payment means; QFT – phone fraud (phreaking); QFZ – other kind of QF); QR – unauthorized copying (QRG – computer games; QRS – other kind of software; QRT – semiconductor topography; QRZ – other kind of QR); QS – computer sabotage (QSH – sabotage with hardware; QSS – sabotage with software; QSZ – other kind of QS); QZ – other kind of computer crimes (QZB – using computer bulletin boards; QZE – theft of information constituting a trade secret; QZS – transfer of information of a confidential nature; QZZ – other kind of QZ) [10].

However, for an ordinary person or financial corporation, the type or form of application of cybercrime or their terminological modifications have little fundamental importance since the result is perceived as a "personal material disaster", financial collapse, or bankruptcy.

4. Conclusion

Of course, today it seems impossible to be fully protected from cyber attacks. However, following at least the minimum safety rules for the online activity will significantly increase the chances that the equipment and codes will not get hacked. Therefore, at the individual level, it is advisable to adhere to the following most optimal basic safety rules:

- use only official software and update it on time;
- do not download software from untrusted sources;
- use antivirus software to work with computers;
- do not share your personal data (card PINs, CVV numbers, account passwords, etc.) with anyone, even if they try to point out the need for such actions in order to resolve a certain issue;
- create complex passwords;
- do not make payment transactions on an open, unsecured Wi-Fi network;
- use two-factor authentication;
- do not open files or emails from suspicious sources;
- do not click on suspicious links and pop-ups;
- do not visit untrusted sites or download any software from such sites;
- do not insert flash drives or external drives into your computer if you do not fully trust their source;
- regularly back up important information;
- keep your gadgets in sight in places where they can be accessed by unauthorized persons.

Taking these security measures will only minimize the possibility of accidental unauthorized entry into devices and systems. However, as experts generally say, it is impossible to provide an absolute guarantee of avoiding hacking [12]. To bring such risks to a minimum, companies are recommended to use the services of cybersecurity specialists with strict compliance with all the instructions designated. It is worth remembering that the world is living in the era of information technology, which means the possibilities of the network are not only a source of opportunities, knowledge, and communication, but also a source of increased danger of being "an open book" if certain individuals are interested in the financial situation of individuals, families, corporations, and any structures.

We believe that the above measures should be used more actively. A comprehensive fight against cybercrime will strengthen the economic foundations of the security of enterprises, institutions, and organizations. Considering the cross-border nature of cybercrime, it is necessary to establish cooperation between law enforcement agencies while investigating cybercrime at the operational level. Creating and ensuring the functioning of a mechanism for resolving jurisdictional issues in cyberspace come as a logical measure for effective and safe functioning in the digital space. In the modern information society, where cyber threats are widespread and will continue to spread, it is important to constantly, systematically, and timely take effective measures to counter cybercrime and improve methods and forms of its prevention. This applies to almost all spheres of public and nation life, business, and socio-humanitarian environment.

Since Ukraine has been on its way to enter the global information space, we are convinced that it is necessary (i) to build a national model for ensuring the cybersecurity of enterprises, institutions, and organizations, including non-governmental ones; (ii) to coordinate efforts and interaction of law enforcement agencies, special services, the judicial system as well as their proper personnel and logistical support, exchange of information on the prevention and fight against cybercrime.

References

[1] Altowaijri, S. (2021). Reducing Cybersecurity Risks in Cloud Computing Using A Distributed Key Mechanism. International Journal of Computer Science and Network Security, 21(9), http://paper.ijcsns.org/07_book/202109/20210901.pdf

[2] Bolgov, V., Gadion, N., Gladun, O. (2015). Organizational and legal support for countering criminal offenses committed using information technologies. Kyiv: National Academy of Prosecutor's Offices of Ukraine. (in Ukrainian).

[3] Cybercrime: problems of struggle and forecasts. (2021). Independent association of banks of Ukraine. (in Ukrainian). http://anticyber.com.ua/article_detail.php?id=140

[4] Kopan, O., Skulish, E. (2012). Dictionary of Cybersecurity Terms. (in Ukrainian).
[5] Gharieb, M. (2021). Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah Al-Mukarramah-Saudi Arabia. International Journal of Computer Science and Network Security, 21(8), http://paper.ijcsns.org/07_book/202108/20210845.pdf
[6] Ishchuk, A. (2018). SPECIFIC FEATURES OF ENGLISH ECONOMIC TERMS. In 5th International Conference Science and Society-Methods and Problems of Practical Application (pp. 25–27). http://ppublishing.org/upload/iblock/e6c/Science-and-society-5.pdf
[7] Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine". (in Ukrainian). https://zakon.rada.gov.ua/laws/show/2163-19#Text
[8] Matveev, V., Nykytchenko, N., Stefanova, N., Khrypko, S., Ishchuk, A., & PASKO, K. (2021). Cybercrime as a Discourse of Interpretations: the Semantics of Speech Silence vs Psychological Motivation for Actual Trouble. International Journal of Computer Science and Network Security, 21(8), 203–211. https://doi.org/10.22937/IJCSNS.2021.21.8.27
[9] McGuire, M., Dowling, S. (2013). Cyber crime: A review of the evidence. Research Report 75. Summary of key findings and implications. University of Surrey. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
[10] Ohnishi, K. (2018). Firms` Strategic Decisions: Theoretical and Empirical Findings, Volume 3. Bentham Science Publishers.
[11] Osipenko, A. (2004). Fighting Crime in Global Computer Networks: International Experience: Monograph. Moscow.: Norma. (in Russian). http://lawlibrary.ru/izdanie50576.html
[12] Shemchuk V. Cybercrime as an obstacle to the development of the information society in Ukraine. scientific notes of Vernadsky Tavrichesky National University. Series: Legal Sciences. 2018. Vol. 29(68), № 6. PP. 119–124. (in Ukrainian). http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_6_23.
[13] Singh, S., Silakari, S. A Survey of Cyber Attack Detection Systems. International Journal of Computer Science and Network Security, vol. 9, No. 5, pp. 1–10. http://paper.ijcsns.org/07_book/200905/20090501.pdf
[14] Stefanova N. (2011). English-language terminolexis of the field of education of the late XX – early XXI century: monograph. Kyiv: Dragomanov National Pedagogical University. (in Ukrainian)

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 Morokhovsky Department of English Philology, Translation and Philosophy of Language, Faculty of Germanic Philology, Kyiv National Linguistic University (Ukraine). Her scientific interests imclude 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

Olena Ishchuk
Doctor Honoris Causa of UACU, Master's Degree in Philological Education. Associate Professor at the Department of General Studies, Ukrainian-American Concordia University (Kyiv, Ukraine). Her scope of interests includes Business English, international management, interpersonal communication.
https://orcid.org/0000-0003-4952-2080

Tetiana Bondar
ORCID iD 0000-0001-6796-0063
PhD (Pedagogy), Associate Professor,
Associate Professor of the Department of Philosophy,
Borys Grinchenko Kyiv University,
13-B, Marshal Timoshenko St., Kyiv, Ukraine,
t.bondar@kubg.edu.ua