Identity of the Suspect in Cyber Sabotage

Submitted: 4 August 2022
Reviewed: 20 October 2022
Revised: 1st March 2023
Accepted: 3rd March 2023

Oleh Peleshchak[*]
https://orcid.org/0000-0002-2785-7464
Roman Blahuta[**]
https://orcid.org/0000-0002-8087-5995
Larysa Brych[***]
https://orcid.org/0000-0002-7079-3726
Nataliya Lashchuk[****]
https://orcid.org/0000-0001-9723-9824
Dmytro Miskiv[*****]
https://orcid.org/0000-0003-3710-0374

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.44518

Abstract

[Purpose] The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.

[Methodology] The research is based on a systematic approach and logical tools (description, analysis, synthesis, induction, deduction, etc.). Special scientific, general scientific, and philosophical methods are applied.

[Findings] The study analyses the possible motives of the suspect in cyber sabotage and unifies classification approaches. Attention is focused on information support for the interrogation of a suspect in cyber sabotage by an investigator to learn the identity of the suspect. Certain features of the sources of obtaining information about a person suspected of committing cyber sabotage are noted. The general characteristics and features of the identity of a cyber sabotage suspect cannot be considered outside the context of other socially dangerous attacks in cyberspace. The development of mechanisms for countering cybercrime in Ukraine continues.

[Value] The practical significance of the study is determined in the list of measures and means proposed by the authors to reduce the risk of cyber sabotages and eliminate their harmful consequences.

Keywords: Criminal Identity. Forensic Characteristics. Cybercrime. Prevention. Cybercrime.

[*] Postgraduate Student, Department of Criminal Procedure and Criminalistic, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: peleshchak8739@yahoo.com.

[**] PhD in Law, Professor, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: ro-blahuta@gmail.com.

[***] Full Doctor in Law, Associate Professor, Head of the Scientific-Research Laboratory, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: lbrych@outlook.com.

[****] PhD in Law, Head of the Department of Criminal Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: nat.lashchuk@aol.com.

[*****] PhD in Law, Lviv Branch, Department of Homeland Security of the National Police of Ukraine, Lviv, Ukraine. E-mail: miskiv5@outlook.com.

PELESHCHAK, O., BLAHUTA, R., BRYCH, L., LASHCHUK, N. & MISKIV, D. *Identity of the Suspect in Cyber Sabotage*. The Law, State and Telecommunications Review, v. 15, no. 2, p. 174-186, October 2023.

INTRODUCTION

Nowadays, cybercrime is the most dynamically developing type of socially dangerous attacks in the world and in Ukraine. Over the past ten years, there has been an increase in this type of crime exponentially. During 2020, more than 5000 cybercrimes were registered in Ukraine, 106 persons involved in criminal proceedings were detained (In 2020, the National Police…, 2021). The prerequisites for this increase are the availability of computer knowledge, a growing level of integration of technologies into the economy and public life, technological progress (improving the technical characteristics of equipment combined with reducing the price of it), insufficient level of security of information processes, cross-border (no state borders in cyberspace), an increase in the Internet, telecommunications, and other types of networks (the ability to connect to them via ordinary telephone lines), improvement of network technologies, an increase in the number of users (their low legal awareness, disregard for the rules of cyber hygiene, non-compliance with the policy of code (password) and information security), corruption component, hyperlatedness (fear of victims losing their reputation, revealing their security schemes, exposing their own illegal actions) etc (DE FRÉMINVILLE, 2020; GETMAN et al., 2019). Cyber threats against unauthorised interference, distributed denial-of-service (DDoS) attacks, the spread of malicious software (including one that can automatically type all alphanumeric combinations based on the principle of a random number generator for setting a password), internet fraud, the establishment of hidden access for the purpose of future control to the use of fake twin sites, simulation programmes, chatbots, cloud technologies, and many others are also being modified. In this context, cyber-attacks on the public sector are also increasing, which, considering modern threats and challenges, slow down positive development trends and threaten both society and the state. Illegal access or distortion of computer information can disrupt the operation of state security systems and lead to material damage and human casualties (RYCHKA, 2019).

Modern information technologies and the latest software not only affect economic processes, and therefore politics and overall society, but also provide new and more advanced opportunities for committing previously unknown offences, or committing traditional crimes by non-trivial methods and means. However, there is a limit of the law that is mandatory for both the real and virtual world (BILENCHUK, 2001). The identity of the criminal is the source of the crime, and therefore, the analysis of thinking, characteristics, and specific features of the person suspected of committing cyber sabotage play an important role in forming the trace picture of this crime. The study is significantly complicated by the lack of an unambiguous assessment of "cyber incidents" in national legislation (usually they are conditionally interpreted as a way of committing), the dispersion of factual and objective information about these individuals in the reports of various law enforcement departments of Ukraine, the hyper-diversity and atypicality of ways and means of committing cyber sabotages (TACIJ et al., 2014). Therefore, the work of law enforcement agencies to detect, investigate, and prevent crimes in this area in a timely manner requires further adequate organisational, managerial, and forensic means and measures to counteract and intensively introduce innovations.

The above causes an urgent need for further study in this area to clarify certain scientific provisions in order to improve the methodology for investigating crimes of this category, establish productive interaction between law enforcement agencies, strengthen criminal legal protection, and criminal liability, require analysis and addition of the arsenal of countering the commission of cyber sabotages (DENYSOVA, 2003; LUTSENKO, 2017; BORYSOVA et al., 2019). Liability for criminal offences in the use of electronic computers (computers), systems and computer networks and telecommunication networks are provided for in Chapter 16 of the Criminal Code of Ukraine. If the violation of automated systems is associated with the commission of more serious crimes (for example, sabotage, espionage, theft of property, etc.), the actions of the perpetrators are qualified according to the totality of crimes (BORYSOVA, 2006). The purpose of the study is to identify means and measures to counteract and prevent cyber sabotage.

MATERIALS AND METHODS

The study applied special scientific, general scientific, and philosophical methods. This allowed comprehensively considering the subject matter. Using the dialectical method, the process of developing criminological knowledge about the identity of a cybercriminal in general and a person suspected of committing cyber sabotage, in particular, was considered. The use of a criminological approach to the investigation of a person suspected of committing cyber sabotage is complex, since it covers sociological, criminal-legal, psychological, and pedagogical aspects of scientific analysis. The use of methods of analysis, synthesis, induction, and deduction identified socio-demographic, criminal-legal, and moral and psychological features of a person suspected of cyber sabotage, forming a list of measures and means of countering and preventing cyber sabotages.

Criminological and criminalistic sources were analysed using various methods of legal interpretation and in the context of the hermeneutical method of scientific knowledge. This facilitated an in-depth analysis of the subject matter. The logical and semantic approach was used to analyse classification systems and types of cyber criminals. The scientific conclusions were confirmed using the statistical method.

The problems of characterising the face of a cybercriminal have been considered by many researchers since the beginning of the 21st century. Some aspects of this problem were investigated by: P.D. Bilenchuk (2001), O.O. Denysova (2003), L. Borysova (2006), K. Titunina (2006), V.B. Shkolnyi (2012), N.S. Kozak (2013), S.V. Yakimova and B.C. Borovikova (2016), O.Yu. Ivanchenko (2019), M.O. Gvozdetska and K.Yu. Izmaylov (2016), V.Yu. Shepitko and V.A. Zhuravel (2017), B.Yu. Chernikov (2018), O.Yu. Dovzhenko (2019), M.I. Maliy and P.D. Bilenchuk (2019), D.O. Rychka (2019), N.L. Pushina (2020), M.W. Kranenbarg, S. Ruiter, J.L. Van Gelder (2021), A.F. Karachka (2017), O.R. Peleshchak (2021).

RESULTS AND DISCUSSION

When qualifying crimes related to computer equipment, it is necessary to consider not only the general rules for qualifying crimes, but also some specifics of crimes inherent only in such acts. The object will be especially important for the qualification, that is, the identity of the criminal and their forensic characteristics. Computer criminals are colloquially referred to as "hackers", "software crackers", and "phreakers". A hacker is a highly qualified IT (information technology) professional who understands the intricacies of computer software. A cracker is an IT professional who hacks security systems (including software protection), software, creates or modifies hacking, and much more. The result of hackers is deliberate cracks, which are programmes that allow hacking software. Software crack is usually suitable for mass production. In fact, a crack is the epitome of a type of hacking, most often it is a general patch (information intended for automatically making certain changes to computer files). In most cases, software crack does not have the source code of the programme, so the disassembler and debugger investigate the programme using special utilities (MAYER LUX & VERA VEGA, 2020). A phreaker is a person who is engaged in phreaking. This term is also used for people who use the phone for their illegal actions in order to psychologically influence the end user.

Recently, phreaking is understood as various ways of hacking electronic systems, such as bank security systems and access control systems. As a consequence of the above, these individuals have special knowledge and practical skills in the field of computer technology and are at least computer users. In a computer information crime against a legal entity, the perpetrator or accomplice (accomplice) is usually an employee of this institution or organisation. These are computer operators, peripherals and communications equipment; programmers; system administrators; electronics engineers; database administrators; network security specialists, civil servants and other persons who have access to computer information and equipment, their networks. Competitors or industrial spies, and professional criminals and cyberterrorists, can pose a serious threat to network security. Representatives of these groups are engaged in illegal activities from corporate espionage to extremely dangerous sabotage of computer systems of vital objects. In recent years, the investigation of the identity of a criminal in global computer networks has faced a significant increase in criminal activity on the part of hackers. Not only in identifying the fact of committing a cyber sabotage after the fact (according to experts, 90% of cases of crime detection are generally due to chance), but also in investigating this type of crime, there are certain difficulties. It is quite difficult to identify, record, and seize criminally significant information when performing investigative actions for use as material evidence (CHERNIKOV, 2018). Most of this information can be obtained by using profiling methods both when identifying a cybercriminal and to prevent illegal actions. Since a wide range of people are involved in cybercrime, the establishment of a database of typical profiles of cyber criminals and the study of their general features allows optimising the process of narrowing the circle of suspects.

Speaking about the personality of criminals, it is important to emphasise that this type of person is characterised by a high level of intellectual development, unusual thinking, professionalism, fanatical attitude to new computer technologies, ingenuity, rich imagination, and secrecy. As a rule, the criminal among the employees of the organisation is an exemplary employee with appropriate training. Such persons have not previously committed any criminal offences. Often these are managers of various ranks who have leadership roles, but are not directly responsible for specific areas of work with computer information. Most often, crimes in the field of computer information are committed by stable criminal groups that are characterised by mobility, high technical equipment, a clear distribution of roles, expressed self-serving motivation and a well-thought-out system for hiding traces of criminal activity (CHERNIAVSKYI et al., 2019). The greatest danger and difficulties for detection and disclosure are criminal groups, which include highly qualified specialists with special knowledge in the field of secret obtaining and protection of computer information. Most of the crimes committed by these subjects remain latent.

The vast majority of offenders are adults, with an almost uniform distribution by age. It should also be noted that the vast majority of those who have committed these types of offences have higher or secondary special education. As for the gender characteristics of the attacker, it can be stated that criminal offences in the field of computer information are committed mainly by men. In the current period, a large number of people, both non-professional and highly qualified specialists, will be involved in the commission of computer crimes. At the same time, all of them have different social status and level of education, which already allows them to be divided into two large groups – these are both people who are in an employment or other employment relationship with the victim, and people who do not have a corresponding connection with the victim. The first group should include employees who abuse their position. These are different types of clerks, security guards, supervisors, people who deal with organisational issues, engineering and technical personnel.

Computer security experts believe that amateur hackers are the most numerous, but the least dangerous. They account for up to 80% of all computer attacks. But these people are not interested in a specific target, but in the attack process itself, and they enjoy overcoming defence systems. For the most part, their actions can be easily stopped, since amateur hackers prefer not to take risks and avoid problems with the law. Most people of this type were connected to computers at school. Knowledge of computer technology is limited to one or two programming languages. The installation of criminal behaviour among amateurs happens spontaneously, mainly under the influence of a random chain of successful and unsuccessful "hacks" of security programmes on other computers. The consolidation of this attitude occurs under the influence of the "authoritative opinion of senior comrades", which they express after communicating with the "newcomer" in the network "lobbies". As the level of professionalization increases, amateurs acquire a deeper, more systematic knowledge of computer technology, programming languages, solid skills and abilities in working with networks, software, etc. This is related to the actual acquisition of higher technical education. They are already specialists. People in this group are psychologically more balanced, have a well-developed system of thoughts and values, but are not yet very ambitious. In most cases, the criminal "career" of such a group of people is transformed from an amateur "career" or developed by entering the criminal environment, for example, with the help and support of "professional" friends. The main areas of criminal activity of "specialists" are network hacking, actions in operations to obtain confidential information using powerful data protection systems, economic and mental espionage.

One of the most important elements for identifying a cybercriminal is motivation, the definition of which can provide information about the needs, interests, and characteristics of the suspect. Motives can be the following: political, ideological (for example, as a form of protest, so-called "hacktivists"); hooligan motives; self-serving (commercial calculation, thirst, material interests); sexual motive; obtaining specific items that have a special value in the cyber world or a higher unofficial social status, competition, technical challenge, struggle between human and artificial intelligence; the desire to have fun, assert themselves, prove intellectual abilities, curiosity, game; research, experiments on the study of software and technical electronic devices, networks, search for weaknesses, opportunities for them use and elimination; manifestations of sadism, painful imagination, pathological predisposition to destructive influence on society and public relations, obtaining moral satisfaction from the scale of destructive consequences; revenge (for example, for troubles at work), personal hostility; negligence, etc. (SHULZHENKO & ROMASHKIN, 2021). Sometimes the motives are complex or complementary to the main ones. The prerequisites for cyber sabotage are the following objective and subjective circumstances:

(1) Wide development of the high-tech industry and significant spread of computer technologies among the population;
(2) Availability of specialities in higher educational institutions that train students with the instillation of subject knowledge, programming skills, and knowledge;
(3) Influence of the family and non-family environment on the process of becoming the culprit of computer information;
(4) Actual impunity of persons who have committed computer crimes due to the high latency of these illegal actions, the lack of proper training of law enforcement officers involved in criminal proceedings on this category of crimes.

No less informative is the professional operation of investigative types of classifications of cyber criminals. For example, depending on their motives, they are divided into: hackers, criminals, vandals (In 2020, the National Police…, 2021). Depending on the purpose of committing a criminal offence, and the scope of application of professional skills, cyber criminals are conditionally divided into four groups: those who "crack" codes and passwords more through curiosity and self-affirmation, trying to find out what will happen for this (usually teenagers, students), by their actions they create serious obstacles to the normal operation of networks and computers; persons who are engaged in targeted theft of new software that is distributed for a fee. Characteristic of this category is the establishment of stable groups with a clear distribution of responsibilities among their members: some crack security codes and passwords, others are engaged in their implementation; computer hooligans who spread computer viruses that destroy software; criminals who hunt for confidential information, sometimes on order, receiving material remuneration for this.

In the specialised literature, there are a large number of other classifications of cyber criminals according to: age characteristics; professional and qualification characteristics (the most difficult to investigate are cases of combining professions); type of labour relations with the affected party; signs of employment; state of health, mental changes; gender characteristics; repeatability of criminal actions (recidivism); individual psychological traits; the ability to access information, the nature of encroachment on it; the method and purpose of committing; social status in society; the scope of crime; the state of awareness of crime actions (often the criminal is not able to fully foresee the consequences of their actions, which depend on many subjective and objective factors. This applies to professional violators of the operating modes of equipment, whose unintentional actions can lead to less serious consequences than a planned cyber-attack); the number of performers, etc. At the stage of preparing for the interrogation of a cyber sabotage suspect, the investigator needs to conduct information support, investigate the suspect's identity and carry out planning. The main tasks of the interrogation are: identification of elements of the composition of cybercrime; establishment of its circumstances, method, motives, accompanying circumstances; identification of signs of cybercrime; establishment of the method of its concealment.

Next, the study considers the investigation of the identity of a suspect in cyber sabotage. Information is to be established by traditional investigative means: biographical data, previous activities (educational, labour); individual psychological characteristics (assigned forensic psychological and/or forensic psychiatric examination, visual observation is conducted, sources of open information are analysed for the study of professional interests, interests, hobbies, attitude to social phenomena, approval of criminal behaviour, etc. (sources of Information: groups in social networks, free ads); special and professional skills (pattern in crime of cyber criminals, which is expressed in certain ways, methods and techniques committing cybercrime, they can be detected by an involved specialist based on the analysis of the technology and method of obtaining illegal remote access (more often cyber criminals prefer to intercept information when transmitting it via telecommunications channels and computer networks, rather than directly entering the premises), establishing important technical data (IP (internet protocol), email address, mobile phone number); features of the subject of encroachment (for example, banking or commercial information); interaction with the victim or the affected organisation; time and place of the crime.

The investigator conducts research and compares data about a person from different sources. Thus, scientific studies on individuals who had information about those who committed cybercrime note that in 31% of cases other people had information about the plans of the criminal; in 64% of cases – colleagues, in 21% – friends, in 14% – family members, in 14% – accomplices (GVOZDETSKA e IZMAYLOV, 2016). Usually, cyber criminals think through their actions in advance and take measures to hide them. If the preparation for the commission of a crime takes place without the involvement of unauthorised persons, the search history in the browser or information from witnesses regarding the search for special literature or special software tools by the suspect may become informative. During the interrogation, as in a normal interview, the investigator should identify contradictions, lies in the testimony, identify the person's attitude to the crime and be prepared for intellectual opposition from the criminal. The investigator and specialist should pay particular attention to the unsystematic unjustified destruction of obstacles (including in cyberspace), the absence of traces in places where logically they should be (staging), the nature of hacking (may indicate penetration from the inside of the room/internal server of the organisation). According to a study by IDG (International Data Group) Corporation, 88% of cases of information theft occur through employees of firms and only 12 % – through external penetration using special means (YAKIMOVA e BOROVIKOVA, 2016).

Therefore, the main danger is caused by internal users (or with their help). They commit 94% of crimes, while external crimes – only 6% (AIKOV e SEIGER e FONSTORCH, 1999). Notably, deliberate destruction of information is most often carried out by former employees or employees of the organisation in order to conceal other crimes or negligence. In cyber extortion, the criminal has access to information that is used when threatening the victim. The peculiarities of the interrogation of a perpetrator of cyber sabotage are the high intellectual level, the special psychological make-up of the interrogators, and the complex technical nature of the questions to be clarified. Recently, there has been a tendency to complicity in group cyber-attacks. Judicial practice shows that 38% acted independently, 62% – as part of organised groups and terrorist communities (SHEPITKO e ZHURAVEL, 2017). The most dangerous due to the ability to organise and commit cyber sabotage are organised groups of corrupt representatives of various state structures, special services that have almost unlimited financial capabilities, independently regulate and control Internet traffic, highly professional, educated, can enjoy the support of legislation and local authorities.

In order to prevent cybercrime, including cyber sabotage, the following technical and organisational measures can be implemented: periodic inspection of equipment for unauthorised access, statistical analysis of traffic to detect anomalies (with the help of a specialist or special software); maintaining a register, database of cyber criminals; introducing mandatory identification and verification of the Internet users; limiting the circle of intermediaries; constant testing and improvement of programmes for the state of protection of users' rights, especially in the field of public services; improving the protection of electronic digital signatures of users; informing internet users about the rules of cyber hygiene, risks and possible cyber threats (including in the cloud environment); establishing rules on the tactics of internet users' actions for typical, atypical and suspicious actions of unauthorised persons in cyberspace (recommendations); establishing technical and other types of restrictions (for example, setting network filters, using a virtual private network), etc. High requirements are also imposed on the investigator of the fact of cyber sabotage, they must have training at the level of a professional programmer or system administrator, be able to use the appropriate software, understand the internal mechanisms of systems and networks, be able to use certified software tools during a search and when collecting physical evidence.

CONCLUSIONS

Cybercrime is becoming more and more global, the latest technologies are turning real criminals into anonymous ones, and the ease of getting rich quickly attracts more and more people to join this criminal activity. Lack of demand for creative potential combined with ignorance of all the consequences of illegal actions – on the one hand, cold professionalism – on the other. These are just common features of cyber criminals. Their technical armament, knowledge, and skills far exceed the capabilities of law enforcement agencies, so improving law enforcement systems is becoming more difficult and expensive. Since the conditions of cyberspace differ significantly from real ones, in order to establish the process of occurrence of criminal intent, its nature, and the degree of public danger of the criminal, there is also a need to classify criminals depending on various subjective and objective factors. Prevention of cybercrime is based on measures aimed at reducing the risk of committing such crimes and neutralising harmful consequences for society and the public and private sectors. Effective counteraction combines a complex of legal (legislative), technical, organisational, and informational measures.

At the legislative level in Ukraine, many issues in the field of countering cybercrime remain unresolved. These are, first of all, gaps in the current legislation in the field of: information technologies, electronic proof, prevention and counteraction to the legalisation of proceeds from cybercrime, and the lack of sufficient investigative and judicial practice in criminal cases on the fact of cyber sabotage and single information and legal space that ensures legal awareness of all structures of society and each citizen separately. Advanced legal regulation can also be provided by: highlighting cyber sabotage and other crimes committed using computer technologies (cyber sabotage, unauthorised collection of information, cyber stalking, cyber investigation) in a separate group of illegal acts in the criminal law, strengthening criminal liability for cybercrime; improving the mechanism for recognising electronic documents and other data as an evidence base in the investigation of cybercrime; clear regulation of interaction between law enforcement agencies. Difficulties in obtaining the necessary amount of information about the identity of the criminal are associated with their high latency, as noted above. These issues are rarely brought to the attention of law enforcement agencies, which allows tracking the characteristics of the criminal introduced in the form of technical developments. However, it is possible to use the above to create a portrait that meets modern realities. Paradoxically, attracting hackers to socially useful work can also help law enforcement agencies, as one of the measures to prevent computer crimes and solve those already committed.

REFERENCES

Aikov, D., Seiger, K. & Fonstorch, W. (1999). *Computer crimes:* A guide to combating computer crimes. Moscow: Mir.

Bilenchuk, P. D. (2001). Questions of social and criminological characteristics of a computer criminal. *State and Regions,* 4, 16-22.

Borysova, L. (2006). Subject (person) of transnational computer crime: forensic and psychophysical aspects. *Current Issues of State and Law,* 1, 76-81.

Borysova, V. I., Ivanova, K. Y., Iurevych, I. V. & Ovcharenko, O. M. (2019). Judicial protection of civil rights in Ukraine: National experience through the prism of European standards. *Journal of Advanced Research in Law and Economics,* 10(1), 66-84.

Cherniavskyi, S.nS., Holovkin, B.nM., Chornous, Y.nM., Bodnar, V.nY. & Zhuk, I.V. (2019). International cooperation in the field of fighting crime: Directions, levels and forms of realization. *Journal of Legal, Ethical and Regulatory Issues,* 22(3), 1-11.

Chernikov, B. Y. (2018). Criminological characteristics of cybercrime. *Young Scientist,* 11(63), 941-944.

De Fréminville, M. (2020). *Cybersecurity and decision makers:* Data security and digital trust. Wiley: ISTE

Denysova, O. O. (2003*). Information systems and technologies in legal activity.* Available at: http://ukrkniga.org.ua/ukrkniga-text/817/.

Dovzhenko, O. Y. (2019). On the question of tactics of interrogation in cybercrime cases. *Scientific Bulletin of the International Humanities University,* 37, 143-145.

Getman, A., Karasiuk, V., Hetman, Y. & Shynkarov, O. (2019). Ontological representation of legal information and an idea of crowdsourcing for its filling. *Advances in Intelligent Systems and Computing,* 836, 179-188.

Government Portal. *In 2020, the National Police exposed more than 5000 cybercrimes.* Available at: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv.

Gvozdetska, M.O. & Izmaylov, K.Yu. (2016). Criminological characteristics of cybercrime: Current state, structure and specifics of committing. *Current Challenges and Achievements in the Field of Cybersecurity,* 2, 52-53.

Ivanchenko, O. Y. (2019). Criminological characteristics of cybercrime, prevention of cybercrime at the national level. *Actual Problems of Domestic Jurisprudence,* 3, 172-177.

Karachka, A. F. (2017). *Technologies of information protection*. Ternopil: National University of Economics.

Kozak, N. S. (2013). Forensic characteristics of persons who commit computer crimes. *Scientific Bulletin of the National University of the State Tax Service of Ukraine (Economics, Law),* 2(61), 186-191.

Kranenbarg, M. W., Ruiter, S. & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology,* 18(3), 386-406.

Lutsenko, O. (2017). Bringing civil servants to liability for disciplinary misconduct in judicial practice of Ukraine, Poland, Bulgaria and Czech Republic. *Journal of Advanced Research in Law and Economics,* 8(1), 103-112.

Maliy, M. I. & Bilenchuk, P. D. (2019). *Cyberspace in the new millennium.* Who are they: cybercriminals? Available at: https://cutt.ly/UZmm0d9.

Mayer Lux, L. & Vera Vega, J. (2020). The crime of cyber espionage: Definition and delimitation. *Revista Chilena De Derecho y Tecnologia, 9*(2), 221-256.

Peleshchak, O. R. (2021). *Survey of the premises in the investigation of cyber diversions*. Madrid: Barca Academy Publishing.

Pushina, N. L. (2020). Forensic characteristics of a person who commits criminal offenses in the field of economic activity with the use of computer technology. *Scientific Notes of TNU named after V.I. Vernadsky,* 31(70), 121-126.

Rychka, D. O. (2019). *Peculiarities of the criminal-law qualification of crimes in the sphere of the use of electronic computers, systems and computer networks and telecommunication networks.* Dnipro: University of the State Fiscal Service of Ukraine.

Shepitko, V. Y. & Zhuravel, V. A. (2017). *Innovative principles of technical and criminalistic support of the activity of criminal justice bodies.* Kharkiv: Apostil.

Shkolnyi, V. B. (2012). Some reasons for the emergence and development of crime in the use of computers. *Law and Society,* 2, 222-227.

Shulzhenko, N. & Romashkin, S. (2021). Types of individual criminal responsibility according to article 25 (3) of rome statute. *Juridical Tribune,* 11(1), 72-80.

Tacij, V. J., Tjutjugin, V. I. & Grodeckij, J. V. (2014). Conceptual model establish responsibility for offense in the legislation of Ukraine (draft). *Criminology Journal of Baikal National University of Economics and Law,* 2014(3), 166-183.

Titunina, K. (2006). Characteristics of computer crimes committed using the Internet (analysis of questionnaires). *Fight against Organized Crime and Corruption*, 21, 307-313.

Yakimova, S.V. & Borovikova, B.C. (2016). Personality of an economic criminal. *Bulletin of the National University Lviv Polytechnic*, 837, 521-527.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET