Pakistan Journal of Criminology
Vol. 15, No. 02, April-June 2023 (165-180)

The Legal Status and Capabilities of Cyber Police in Ukraine: The Reasons for the Existence of Frauds with the Use of IT Technologies

Oleksandr Punda[1], Mykola Vavrynchuk[2], Olha Kohut[3],
Stepan Kravchuk[4] & Mykhailo Prysiazhniuk[5]

Abstract

The relevance is determined by the prevalence of cybercrime, which has now acquired an international character, which in turn necessitated the development of scientifically based approaches to combating such a negative phenomenon. The purpose is a systematic review of scientific research, normative legal acts, reports and strategies in order to identify the problems of countering cybercrime in Ukraine. According to the Report of the National Police of Ukraine on the results of work in 2021, positive trends are noted in the work of the cyber police of Ukraine, given that in 2021 the level of detection of cybercrimes increased significantly. The publication examines the practical problems of the Cyber Police Department of the National Police of Ukraine, as well as options for countering cybercrime in Ukraine.

Keywords: National Police of Ukraine, Cybercrime, Cyberspace, Information and Communication Technologies, Internet.

Introduction

The 21st century is characterized not only by the wide development of information and communication technologies but also by the increase of their users, in particular the Internet. Unfortunately, such positive changes have led to the spread of cybercrimes, which in some places can cause significant material damage. D.R. Srivastava and R. Koolwal (2015) state that currently the negative phenomenon of cybercrime has acquired a global character. It is the Cyber Police Department of the National Police of Ukraine that is called upon to counter cybercrime and fight against this negative phenomenon (Yaroshenko and Tomashevski, 2021). It is difficult to overestimate the importance of this

[1]Department of Law, Khmelnytskyi National University, 29016, 11 Instytutska Str., Khmelnytskyi, Ukraine. oleksandr.punda@ukr.net
[2]Department of Law, Khmelnytskyi National University, 29016, 11 Instytutska Str., Khmelnytskyi, Ukraine. mykola.vavrynchuk@proton.me
[3]Department of Law, Khmelnytskyi National University, 29016, 11 Instytutska Str., Khmelnytskyi, Ukraine. olha.kohut@protonmail.com
[4]Department of Law, Khmelnytskyi National University, 29016, 11 Instytutska Str., Khmelnytskyi, Ukraine. stepan.kravchuk@outlook.com
[5]Department of Law, Khmelnytskyi National University, 29016, 11 Instytutska Str., Khmelnytskyi, Ukraine. mykhailo.prysiazhniuk@ukr.net

Department for the cybersecurity of Ukraine. L.BelliandC. Sappa (2017) state that the state regulatory policy in many countries aims to encourage the so-called Internet intermediaries between the owners of the respective websites and their users to take active measures to comply with the implementation of national legislation, a wide range of violations of which is available on the Internet: from copyright infringement rights and privacy to illegal hate speech and child pornography.

T.V. Bilobrov (2020) comprehensively examined the status of cyber police in Ukraine, but only in the administrative and legal aspect. O.A. Samoilenko (2020) published an educational and methodological manual dedicated to the detection and investigation of cybercrimes. The Ukrainian researchers O.V. Artemenko and R.V. Bidonko (2017) highlighted the specifics of activities in cyberspace and the specifics of investigating crimes committed with the use of IT technologies and devoted an article to the organization of activities of cyber police of Ukraine. M.Sh. Hashim (2017) considered the emerging trends of cyber fraud in Malaysia. M. Fahleviet al. (2019) described the state of cybercrime in Indonesia. S.O. Abu et al. (2018) looked into the issues of cyber fraud trends in Nigeria. The study of victims of cyber fraud is devoted to the work of C.Cross and D.Mayers (2021). I.A. Boitan (2020) reviewed the guidelines and reports recently published by the International Monetary Fund, the World Bank, the European Central Bank, the European Commission, the Big Four auditing companies, and research centres in order to analyse cybersecurity challenges.

The purpose is a systematic review of scientific research, legal acts, in particular – Convention on Cybercrime (2005), Criminal Code of Ukraine (2001), Law of Ukraine "On the National Police"(2015), Law of Ukraine "On amendments to certain legislative acts of Ukraine regarding simplification of pretrial investigation of certain categories of criminal offenses"(2018), reports and strategies, namely –Report of the National Police of Ukraine on the results of work in 2021 (2021), Order of the Cabinet of Ministers of Ukraine "On approval of the Strategy for the development of the system bodies of the Ministry of Internal Affairs for the period until 2020"(2017) in order to identify the problems of countering cybercrime in Ukraine. The following task was set:

– to consider the regulatory and legal regulation of the Cyber Police Department of the National Police of Ukraine;

– to investigate the types of cybercrimes provided for by the criminal legislation of Ukraine;

– analyse the current state of cybercrime in Ukraine;

– identify practical problems of combating cybercrime in Ukraine.

Materials and Methods

The study of the legal status of the cyber police, the state of cybercrime and the fight against crimes committed in Ukrainian cyberspace had three stages:

– at the preparatory stage, was collected and analysed theoretical sources, normative legal acts, in particular, Convention on Cybercrime (2005), Criminal Code of Ukraine (2001), Law of Ukraine "On the National Police"(2015), Law of Ukraine "On amendments to certain legislative acts of Ukraine regarding simplification of pretrial investigation of certain categories of criminal offenses"(2018), reports and strategies, namely – Report of the National Police of Ukraine on the results of work in 2021 (2021), Order of the Cabinet of Ministers of Ukraine "On approval of the Strategy for the development of the system bodies of the Ministry of Internal Affairs for the period until 2020" (2017).

– the main stage of the study began with familiarization with the provisions of the Law of Ukraine "On the National Police"(2015) in the aspect of normative and legal regulation of the status of cyber police in Ukraine, which made it possible to ascertain the general nature of this legislative act in the context of the activities of the Cyber Police Department of the National Police of Ukraine. The authors reflected in the work special criminological measures to prevent cyber fraud.

– at the final stage of the research, were summarized the considered material and systematically outlined the features of the fight against cybercrime and the current state of this negative phenomenon in Ukraine.

The classification of cybercrimes in the Ukrainian legal space, which allowed to identify violations of the well-known rules of formation of classifications, because the correct approach is when one criterion divides the relevant concepts into groups, was noted. In this regard, it was proposed to divide cybercrimes into groups according to the criterion "according to the method of commission provided for in the criminal law". Also, at the main stage, were reflected the key provisions of the Report of the National Police of Ukraine on the results of work in 2021 (2021) on cyber police activities and cybercrime trends in Ukraine in 2021. It is noteworthy that the insufficient number of professional cyber police officers is a common phenomenon not only in Ukraine, but also abroad.

Results

The main legislative act that regulates the activities of the cyber police in Ukraine is the Law of Ukraine "On the National Police". In particular, in Art. 13 Law of Ukraine "On the National Police"(2015), entitled "General police system", in Part 3, which provides for the composition of the National Police, the cyber

police as a separate unit are not even mentioned –its activities in the system of the National Police of Ukraine are obviously covered by clause 7 of Part 3 of Art. 13 of the Law: other subdivisions, the activities of which are aimed at fulfilling the tasks of the police or ensuring its functioning, the decision on the creation of which is taken by the head of the police in agreement with the Minister of Internal Affairs. It is well known that the activities of the cyber police are related to the investigation of cybercrimes, and therefore a correct understanding of this type of crime, their system, and classification is of particular importance. According to the Convention on Cybercrime (2005), cybercrimes are divided into the following categories:

– offences against confidentiality, integrity, and availability of computer data and systems;

– offences related to computers;

– offences related to content;

– offences related to the violation of copyright and related rights.

T. Kharebava (2017) proposes to divide the cybercrimes provided for by the Criminal Code of Ukraine (2001) into the following groups: 1) criminal crimes committed with the help of computer technologies (violation of copyright and related rights (Art. 176); fraud (Part 3, Art. 190); 2) illegal actions with transfer documents, payment cards, bank accounts (Art. 200); 3) illegal collection of information constituting a commercial or banking secret (Art. 231); 4) importation, production, sale, and distribution of pornographic materials (Art. 301); 5) criminal crimes, in the field of using computers, systems, and networks(Art. 361); 6) creation of malicious software or technical means (Art. 361-1); 7) unauthorized sales or distribution of information with limited access (Art. 361-2); 8) unauthorized actions with information processed by computers (Art. 362); 9) violation of the rules of computer operation (Art. 363); 10) obstruction of work computers by distributing electronic messages (Art. 363)

The authors have serious comments about the above proposed system of classification of cybercrime in the national legislation of Ukraine. According to the authors, given the entry into force of the Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine concerning the simplification of pre-trial investigation of certain categories of criminal offences" (2018), the concept of "crime" was transformed into the concept of "criminal offence". The Criminal Code of Ukraine (2001) provides for a separate method of committing such criminal crimes, such as: fraud –"through illegal operations using electronic computing equipment"; illegal possession of a vehicle –"using electronic devices

to interfere with the work of technical protection means" (Kharebava, 2017; Beretta and Cencini, 2020).

T.Kharebava (2017) also found such a layer of crimes on the Internet, which are considered sexual harassment in international (in particular, British and American) legislation. Authors remind that Art. 156of the Criminal Code of Ukraine (2001) provides for criminal liability for molesting a child for sexual purposes. The provision of Part 1 of this article provides for a special way of committing this criminal offence (crime) – with the use of information and telecommunication systems or technologies. At the same time, Article 154 of the Criminal Code of Ukraine (2001), which, according to its content, is a kind of manifestation of sexual harassment and has the title "Forcing sexual intercourse", does not provide for a special way of committing it, while, obviously, this type of criminal crime can be done on the Internet.

The classification of cybercrimes proposed by T.Kharebava (2017) also contains a mention of a special way of committing such a criminal crime –spreading appeals on the Internet. It is also a well-known fact that copyright infringement on the Internet is a fairly common type of cybercrime. Turning to Art. 176 of the Criminal Code of Ukraine (2001) under the title "Breach of copyright and related rights", the authors can state two features of understanding this type of criminal crime as a type of cybercrime. The first feature is related to the subject of Art. 176, because among other subjects (works of science, literature, and art) of the criminal crime "Breach of copyright and related rights" the legislator included computer programs and databases. The second thing is the absence of a traditional, special way of committing this criminal offence on the Internet or cyberspace. Part 1 of Art. 176 indicates the following method of committing a criminal crime –"on audio and video cassettes, diskettes, other information carriers". It is obvious that, most likely, the category "other media" is most suitable for copyright and related rights violations on the Internet. At the same time, another option is possible, the so-called "two-stage", when the violation of copyright and related rights occurs as follows – first, the objects of copyright and related rights are copied onto audio and video cassettes, diskettes, and then – reproduced, distributed in Internet networks.

Also, in this context, the authors would like to note that Article 177 of the Criminal Code of Ukraine (2001) "Infringement of rights to an invention, utility model, industrial design, topography of an integrated microcircuit, plant variety, rationalization proposal" does not contain any mention of any special methods of committing in cyberspace at all. However, obviously, this type of criminal crime can also be classified as cybercrime. In general, the authors would

like, summarizing the issue of the system of cybercrimes in the Ukrainian legal space, to express their disagreement with the widespread doctrinal approach, when in fact scientists divide cybercrimes in Ukraine into two groups: first provided for in Chapter XVI of the Criminal Code of Ukraine (2001), entitled "Criminal offences in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks"; second is criminal crimes, the commission of which is one way or another connected with cyberspace.

The main is that scientists who are supporters of this approach, in particular, T.Kharebava (2017), do not take into account, referring to the first group, in fact, all criminal crimes provided for in Chapter XVI of the Criminal Code of Ukraine (2001), the criterion of separation, which is the guiding principle in the formation of the correct classification. According to the approach proposed by T.Kharebava (2017), it is obvious that the first group of cybercrimes is singled out on the basis of the generic object, while in the second group, the Ukrainian researcher combined according to the "residual" principle – all other criminal crimes that can theoretically be committed in cyberspace. According to the generally accepted scientific rules for the formation of classifications, the correct approach is when one criterion divides the relevant concepts into groups.

In order to solve the situation with the cybercrime system in the Ukrainian legal space, a classification is proposed, provided for by criminal legislation and defined by a specific way of committing it with the help of information and communication technologies (for example, fraud committed through illegal operations using electronic computing equipment, or illegal possession of a vehicle using electronic devices for interfering with the work of technical protection means) and those for which no special way of committing a crime related to cyberspace is mentioned (coercion to sexual intercourse or violation of the rights to an invention, utility model, industrial design, topography of an integrated microcircuit). The approach proposed by the authors to the classification of cybercrimes in the Ukrainian legal space is innovative, and therefore can serve as a basis for scientific discussions and further doctrinal research.

Regarding the current number of criminal crimes in the cyberspace of Ukraine, it should be mentioned Report of the National Police of Ukraine on the results of work in 2021 (2021). It is noteworthy that the Report recognizes the fight against cybercrime as a priority task of the National Police in 2022. The improvement of the organizational and legal foundations of the fight against cybercrime was defined as one of the necessary steps in combating crime also in the Order of the Cabinet of Ministers of Ukraine "On approval of the Strategy for

the development of the system bodies of the Ministry of Internal Affairs for the period until 2020" (2017).Understanding such a concept as "fighting cybercrime" in Report of the National Police of Ukraine on the results of work in 2021 (2021) is interpreted through the prism of combating criminal offences committed in the field of high information technologies. Such criminal offences are detailed and it is indicated that, first of all, they include frauds carried out on the Internet, related to bank cards and the creation of a safe cyberspace.

Report of the National Police of Ukraine on the results of work in 2021 (2021) contains important information about the total number of cybercrimes committed in 2021, namely, the Report states that in 2021 almost twice as many crimes committed using high information technologies were documented as in the previous year. Analysing the dynamics of such criminal offences, the Report informs that the number of crimes in the banking sector has increased by almost one and a half times, and by a third – in the field of computer systems. Nevertheless, according to the Report of the National Police of Ukraine on the results of work in 2021shows a trend towards an increase in the detection of cybercrimes – in 2021, this indicator doubled. Report of the National Police of Ukraine on the results of work in 2021 reports that the number of international police operations at the initiative of employees of the cyber police unit of Ukraine in 2021 was 9. Also, Ukrainian cyber police officers took part in 8 international operations at the invitation of colleagues. It is important to note that citizens of Ukraine actively appealed to cyber police officers in 2021 –over 190000 appeals from citizens were registered during this period. Mostly, potential victims of cybercrime use telephone communication for such appeals, however, the electronic form of citizen appeals is also popular.

As for the reasons for the existence of fraud in the use of IT technologies in Ukraine, first of all, it is worth highlighting the problem of proper training of personnel, which is common not only in Ukraine, but also in other countries. Summarizing the material presented, the authors would like to note positive trends regarding the increase in the number of solved cybercrimes in Ukraine in 2021. At the same time, the problems of combating cybercrime remain widespread not only in Ukraine, but also abroad.

Discussion

The issue of cyber police activity was the subject of consideration in a number of scientific publications. First of all, researchers pay attention to the prevalence of cybercrime at the international level and its global nature. J.M. Drew and L. Farrell (2018) state that the prevalence and impact of cyber fraud continues to grow exponentially due to new and more innovative methods

developed by offenders to find and exploit victims for their own financial rewards. Traditional police crime response methods have proven largely ineffective in this context, as offenders are usually outside the police jurisdiction of their victims (Kaplina and Sharenko, 2020).M. Fahlevi et al. (2019) rightly believe that the development of information technologies, and especially the Internet, has caused significant social, economic and cultural changes. Such changes have both positive and negative character. On the one hand, information technologies simplify access to information, speed up access to it. On the other hand, the development of Internet technologies leads to the emergence of new cybercrimes committed through the Internet. M. Fahlevi et al. (20219) rightly note that cybercrime is currently a global problem. A significant space for committing cybercrimes exists in developed countries, where large companies, especially e-commerce companies, carry out their activities, which is associated with a high risk of theft of customer data, account data and payments from customers (Sakhipov et al., 2022).

J.M. Drew andL. Farrell (2018) understand cyberfraud as a subset of cybercrime, which researchers divide into two categories: the first category is targeting computers or other information and communication technologies (illegal access, illegal interception, data tampering, system tampering, etc.) In general, these crimes can be considered as attacks on computer hardware or other information and communication technologies (Bapiyev et al., 2021). The second category of cyberfraud crimes includes those types of criminal offences, where computers or information and communication technologies are an integral part of the crime. This category of cybercrime is also characterized by the goal of obtaining financial benefit (e.g.,inheritance fraud, investment fraud and fraudulent financial transactions) (Kozii, 2023).

D.R. Srivastava and R. Koolwal (2015) distinguish the following types of cybercrime as cyber-terrorism, computer viruses, cyberstalking, identity theft, etc.M. Fahlevi et al. (2019) propose to divide fraud into two types by subject composition: employee fraud (perpetrated by employees working in a specific organization); management fraud (perpetrated by company management and usually aimed at using financial reports or transactions with funds in order to level cooperation with counterparties).

V.V. Bereza (2018) rightly notes that the main difference between these concepts is that the term “cybercrime” in its meaning includes crimes that are committed both with the use of computer equipment and information technologies and global networks. At the same time, obviously, the term “computer crime” is limited to the understanding of those crimes committed against computers and computer data (Mikhailov et al., 2020).

Some types of cybercrimes were also the subject of consideration by subsequent researchers. P. Basu et al. (2021) define online sexual harassment as unwanted sexual behaviour on any digital platform that is recognized as a form of sexual violence that can make a person feel threatened, exploited, coerced, humiliated, sexualized or discriminated against. P. Basu et al. (2021) argue that it is possible to use this understanding of the concept of "sexual harassment on the Internet" to create models that could automatically detect such socially dangerous behaviour on the Internet, prohibiting offending users from publishing such content in the future, without waiting, until other users report such content. This will create a safe space in social networks. The main problem is a lack of a rigid set of rules or a code of conduct in social networks, which makes it impossible to distinguish jokes from more harmful comments (Sandra and Lumbangaol, 2021; Sandra et al., 2021).

M. Bruno (2019) considers cyber fraud using e-mail by a person other than the one to whom the e-mail belongs to be dangerous, not only because of the difficulties in identifying and protecting personal data, but also because of the risk of high financial losses. A well-known way of committing fraud is the so-called forgery of identification using a fake signature of an individual. A type of identity spoofing when committing cyber fraud is the use of an e-mail by someone other than the person to whom the e-mail belongs (Bedelov et al., 2021). M. Bruno (2019) believes that cyber fraudsters of the new generation, in order to increase the probability of achieving their criminal goals, will use two methods of committing the considered type of crime –traditional and so-called innovative.

A separate aspect of considering the problems of cybercrime is the question of potential victims of cybercrime and their role in preventing the commission of this type of criminal offence. J.M. Drew and L.Farrell (2018) produced the thesis that quite often the reduction in the prevalence of cybercrime depends on the self-defence of potential victims against this type of crime. C.M. Millman et al. (2017), also draw attention to such a problem of the investigation of criminal offences on the Internet as the online nature of the complaints of victims, which may not be taken seriously by the relevant human rights authorities. The following researchers dealt with issues of combating cybercrime, considered practical problems of investigation and prevention of cybercrime. R. Broadhurst et al. (2014) rightly point out that, as a rule, cyber fraud is the work of skilled technicians who apply knowledge of information and communication technologies through the computer and the Internet for criminal activities. In this aspect, S.O. Abu et al. (2018), specify that the subjects of cyber fraud can be both individuals and groups of individuals, as well as organizations, and even states. B.O. Folashade and K.A. Abimbola (2013) considers that a characteristic feature of

cyber fraud is that the legality of a criminal case in this area is difficult to prove. And first of all, the solution to this problem is related to the qualification of the cyber police investigator, who must have proper training, be an expert in forensic computer science, because it is the cyber police investigator who is responsible for detecting, collecting, documenting, preserving, analysis, research, and submission of evidence from computer devices, networks, and other electronic devices to prove the presence of the crime of cyber fraud before the court proceedings (Cointet, 2022; Striltsiv and Fedorenko, 2022).

I. David and S. Karl (1995) note the cumbersomeness of conducting appropriate investigative actions and the process of investigating cyber fraud, because, as a rule, such an investigation requires conducting a forensic digital examination to track, detect, and in some cases –prevent the commission of this type of crime. Researchers also focus on the need for appropriate training and qualification level of cyber police investigators, and even suggest introducing additional higher education for relevant cyber police personnel – majoring in accounting or finance. The classification of cyber-attacks proposed by the Institute of International Finance (2017) has four groups: 1) cybercrime (the determining factor is the motive – financial benefit, for example – to steal money); 2) cyberespionage (the decisive goal is to obtain information about another organization, for example, political, financial, capitalist, information on market shares); 3) cyberattacks of a hacker nature (its main form is the theft of information for a specific purpose); 4) cyberwar (attempts of a state or a transnational organization to compromise/force the victim to take certain actions with the help of a cyberattack). Specialists of the Institute of International Finance emphasize that any attack on critical components of the financial system or service system may have a direct or indirect impact on the security of these objects and threaten either the stability of the financial system or the financial security of its participants.

D. Harkin et al. (2018) conducted an original, empirical study using a questionnaire method (survey, interview) with the participation of specialized cybercrime units in Australia in order to identify the problems that employees of these units face in practice. Thus, Australian researchers identified three main problems of combating cybercrime in this region: 1) the fact that cybercrime has acquired a global character and has become a widespread social problem, the workload of employees of specialized cybercrime units in Australia has increased; 2) lack of development of appropriate resource provision of the relevant units in proportion to the growth in demand for cyber police services; 3) insufficient level of skills, and training of employees of cyber police units, taking into account the complexity of combating cybercrime (Barlybayev and Sharipbay, 2015).

The statement of D. Harkin and Ch. Whelan (2022) that special training of cyber police officers should be carried out taking into account the specifics of the positions held by the relevant officers is also correct. Such positions are divided into certain groups, in particular: senior management and senior officers; ordinary investigators; investigative specialists and civilians in cybercrime units (Shapoval et al., 2018).

S.O. Abu et al. (2018) are convinced that the difficulties of investigating cybercrimes, in particular cyber fraud, are primarily related to the lack of special computer and digital forensic education among cyber police officers. Infrequent or poor-quality holding of specialized training, seminars and conferences for such workers, Nigerian researchers also attribute it to the reasons for the non-disclosure of cybercrimes. Nevertheless, S.O. Abu et al. (2018) believe that the personnel of the relevant companies that are in the group of increased risk of cybercrime (in particular, those that conduct electronic financial transactions, such as e-business, e-commerce, electronic payments, etc.) should have an appropriate level of knowledge of computer forensics education and regularly attend relevant training, seminars, conferences in order to update their knowledge, skills and competence in this field. T.V. Bilobrov (2020) notes that the lack of competitive Ukrainian software products and the lack of access to international software databases affect the effectiveness of cyber police activities in Ukraine.

G.V. Nedzelska (2022) has developed a system of special criminological measures to prevent fraud. She suggests optimizing economic security services operating at a specific enterprise, improving the work of services responsible for internal audit work, verifying employee data when hiring, promptly notifying relevant law enforcement agencies of suspected corporate fraud. The scientific works discussed above have both theoretical and practical significance for the Ukrainian doctrine, which is devoted to the issues of cybercrimes and the legal status of cyber police. At the same time, it is worth paying attention to the fact that the activities of the cyber police as a structural unit of the National Police of Ukraine, especially in recent years, have not been considered by researchers so often.

Conclusions

The work includes a systematic analysis of theoretical sources, legislative acts and reports devoted to the legal problems of combating cybercrime and the legal status of the Cyber Police Department of the National Police of Ukraine. The publication focuses on the fact that, in view of the entry into force of the Law of Ukraine “On amendments to certain legislative acts of Ukraine regarding simplification of pretrial investigation of certain categories of criminal

offenses" (2018), the correct concept for characterizing cybercrimes in Ukraine should be considered "criminal offences in the field of cybersecurity". The authors proposed for the first time to classify cybercrimes in the national legislation of Ukraine according to the method of commission provided for in the criminal law. The data of the Report of the National Police of Ukraine on the results of work in 2021 (2021) are important for the study, it is possible with their help to draw a principled conclusion about the state of cybercrime in Ukraine over the last year: the total number of cybercrimes has a tendency to increase with a simultaneous increase in the detection rate of this type of criminal offence almost double.

In general, when answering the question of why fraud with the use of IT technologies did not disappear with the introduction of a new cyber service, several reasons can be singled out. First of all, it should be noted that the development of information technologies significantly expands the types of cybercrimes and accelerates their occurrence. Information technologies are developing so quickly that the relevant law enforcement structures simply do not have time to react properly. The second reason for the existence of fraud with the use of IT technologies should be considered the problems of the organizational activity of the cyber police, related to the improvement of the qualifications of the personnel of this law enforcement body and adequate funding. It is also worth keeping in mind that the effective fight against cybercrime also depends on preventive measures, which should be applied, first of all, to potential victims who may suffer from cybercrimes (in particular, this applies to employees of large financial institutions). It is possible to recommend to companies conducting electronic financial operations, such as electronic business, electronic commerce, electronic payments, in order to prevent cybercrimes against them, to properly protect personal data, bank accounts from a technical aspect. In general, it can be stated that the effective fight against cybercrime is currently a problem not only in Ukraine, but also in the whole world.

References

Abu, S.O., Lateef, O.M. &Echobu, J. (2018). Determinants of Cyber Fraud Investigation in Nigeria. *Accounting and Taxation Research*, 2(2), 1-14.

Artemenko, O.V. &Bidonko, R.V. (2017). Cyber Police of Ukraine. Organization of Activity and Prospects of Development. *Law and Society*, 1(2), 116-119.

Bapiyev, I., Kamalova, G., Yermukhambetova, F., Khairullina, A., & Kassymova, A. (2021). Neural network model of countering network cyber attacks using expert knowledge. *Journal of Theoretical and Applied Information Technology*, 99(13), 3179-3190.

Barlybayev, A., &Sharipbay, A. (2015). An intelligent system for learning, controlling and assessment knowledge. *Information (Japan)*, 18(5), 1817-1827.

Basu, P., Roy, T.S. & Tiwari, S. (2021). Cyber Police: Classification of Cyber Sexual Harassment. *Progress in Artificial Intelligence*, 2021, 701-714.

Bedelov, K., Bidaibekov, Y., Grinshkun, V., Bostanov, B., & Koneva, S. (2021). The effective use of telecommunication cloud services for the training of future computer science teachers. *World Transactions on Engineering and Technology Education*, 19(4), 398-403.

Belli, L. &Sappa, C. (2017). The Intermediary Conundrum: Cyber-Regulators, Cyber Police or Both? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(3), 183-198.

Beretta, E., &Cencini, A. (2020). Double-entry bookkeeping and balance of payments: the need for developing a new approach. *Insights into Regional Development*, 2(3), 610-629.

Bereza, V.V. (2018). *On the Determination of Cybercrime as an Object of Counteraction in Activity.*Kharkiv: Kharkiv National University Internal Affairs.

Bilobrov, T.V. (2020). *The Administrative and Legal Status of the Cyber Police Department of the National Police of Ukraine.* Kyiv: National Academy of Internal Affairs.

Boitan, I.A. (2020). Cyber Security Challenges through the Lens of Financial Industry. *International Journal of Applied Research in Management and Economics*, 2(4), 33-38.

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime. *International Journal of Cyber Criminology*, 8(1), 1-20.

Bruno, M. (2019). Impersonation Fraud Scenarios: How to Protect, Detect and Respond., 3(1), 6-13.

Cointet, J.P. (2022). Assessing intolerance, the level of protest on the internet and the impact of botfarms on political life in modern France from a sociological standpoint. *European Chronicle*, 7(2), 35-44.

Convention on Cybercrime. (2005). Retrieved from: https://rm.coe.int/1680081561

Criminal Code of Ukraine. (2001). Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text.

Cross, C. &Mayers, D. (2021). Scambaiter Narratives of Victims and Offenders and Their Influence on the Policing of Fraud. *Policing: A Journal of Policy and Practice*, 15(4), 2148-2164.

David, I. & Karl, S. (1995). *Computer Crime: A Crime Fighter's Handbook*. Sebastopol: OReilly.

Drew, J.M. & Farrell, L. (2018). Online Victimization Risk and Self-Protective Strategies: Developing Police-Led Cyber fraud Prevention Programs. *Police Practice and Research*, 19(6), 537-549.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D. &Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *ICENIS*, 125, article number: 21001.

Folashade, B.O. &Abimbola, K.A. (2013). The Nature, Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria- Kaduna State, Nigeria. *American International Journal of Contemporary Research*,3(9), 98-114.

Harkin, D. & Whelan, Ch. (2022). Perceptions of Police Training Needs in Cybercrime. *International Journal of Police Science & Management*, 24(1), 66-76.

Harkin, D., Whelan, Ch. & Chang, L. (2018). The Challenges Facing Specialist Police Cybercrime Units: An Empirical Analysis. *Police Practice and Research*, 19(6), 519-536.

Hashim, M.Sh. (2017). Cyber-Related Fraud Incidents in Malaysia. A Seven-Year Analysis of MyCERT Data. *AsociatiaRomanapentruAsigurareaSecuritatiiInformatiei*, 6(2), 9-16.

Institute of International Finance. (2017). *Cyber Security & Financial Stability: How Cyberattacks Could Materially Impact the Global Financial System*. Washington: Institute of International Finance.

Kaplina, O., &Sharenko, S. (2020). Access to justice in Ukrainian criminal proceedings during the covid-19 outbreak. *Access to Justice in Eastern Europe*, 3(2-3), 115-133.

Kharebava, T. (2017). *The Difference of IT Business from Cybercrime. Not to Be Confused*. Retrieved from:

https://uba.ua/documents/events/2017/20170407/Presentations/Kharebav%D0%B0Tetyana.pdf

Kozii, V. (2023). Criminal liability for illegal possession of cryptocurrency in Ukraine. *Social and Legal Studio*s, 6(1), 33-40.

Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding Simplification of Pretrial Investigation of Certain Categories of Criminal Offenses". (2018). Retrieved from: https://zakon.rada.gov.ua/laws/show/720-20?lang=en#Text

Law of Ukraine "On the National Police (2015). Retrieved from: https://www.rightofassembly.info/assets/downloads/2015_Law_on_the_National_Police.docx

Mikhailov, P.G., Kassimov, A.O., & Umbetkulov, Y. (2020). Systems of monitoring and control of emergency situations in facilities and territories of the republic of kazakhstan. In: *2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020* (article number: 9271391). Vladivostok: Institute of Electrical and Electronics Engineers.

Millman, C.M., Winder, B. & Griffiths, M.B. (2017). UK-Based Police Officers' Perceptions of, and Role in Investigating, Cyber-Harassment as a Crime.*International Journal of Technoethics*, 8, 87-102.

National Plan to Combat Cybercrime. (2013). Retrieved from: https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime.pdf.

Nedzelska, G.V. (2022). Special Criminological Measures to Prevent Fraud by an Organized Group. *Juridical Scientific and Electronic Journal*, 3, 211-213.

Order of the Cabinet of Ministers of Ukraine "On approval of the Strategy for the development of the system bodies of the Ministry of Internal Affairs for the period until 2020". (2017). https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80?lang=en#Text

Report of the National Police of Ukraine on the Results of Work in 2021. (2021). Retrieved from: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf

Sakhipov, A., Yermaganbetova, M., Latypov, R., & Ualiyev, N. (2022). Application of blockchain technology in higher education institutions. *Journal of Theoretical and Applied Information Technology*, 100(4), 1138-1147.

Samoilenko, O.A. (2020). *Detection and investigation cybercrimes.*Odesa: TES.

Sandra, L., &Lumbangaol, F. (2021). When Homecoming is not Coming: 2021 Homecoming Ban Sentiment Analysis on Twitter Data Using Support Vector Machine Algorithm. In: *8th International Conference on ICT for Smart Society: Digital Twin for Smart Society, ICISS 2021 - Proceeding*. Virtual, Bandung: Institute of Electrical and Electronics Engineers.

Sandra, L., Trisetyarso, A., Ramadhan, A., Abdurachnan, E., Lumbangaol, F., &Isa, S.M. (2021). Social Network Analysis Algorithms, Techniques and Methods. In: *2021 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation, ICAMIMIA 2021 - Proceeding* (pp. 182–189). Surabya: Institute of Electrical and Electronics Engineers.

Shapoval, R., Bytiak, I., Khrystynchenko, N., &Solntseva, K. (2018). Problematic issues of the administrative and legal status of the police in the baltic states (Lithuania, Latvia, Estonia). *Journal of Advanced Research in Law and Economics*, 9(1), 295-306.

Srivastava, D.R. &Koolwal, R. (2015). Cyber Crime and its Impact on Business and Social Sector: A Review. *Ascent International Journal for Research Analysis*, 1(1), 1-12.

Striltsiv, O., &Fedorenko, O. (2022). Problems of legal regulation of the use of artificial intelligence technologies by the National police of Ukraine. *Scientific Journal of the National Academy of Internal Affairs*, 27(1), 30-39.

Yaroshenko, O.M., &Tomashevski, K.L. (2021). The impact of COVID-19 on labour and social security relations: Rule-making experience of belarus and Ukraine. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(2), 211-221.