Combating Internet Fraud through Operative-Search Measures

Submitted: 8 September 2023
Reviewed: 26 February 2024
Revised: 15 March 2024
Accepted: 18 March 2024

Article submitted to peer blind review

Samat Shaisultanov[*]
https://orcid.org/0009-0000-4297-6982
Talgat Akimzhanov[**]
https://orcid.org/0009-0001-0402-7441
Boris Abdrakhmanov[***]
https://orcid.org/0009-0000-8838-5459
Ardak Bazarlinova[****]
https://orcid.org/0009-0005-9050-3887
Aida Bazarlinova[*****]
https://orcid.org/0009-0006-2042-7089

DOI: https://doi.org/10.26512/lstr.v16i2.50740

Abstract

[Purpose] Currently, the rapid development of Internet technologies leads to an increase in the number of fraud-related offences, which requires effective ways to prevent and detect them. The purpose of the study was to determine the essence, features, and problems of operative-search counteraction to Internet fraud.

[Methodology] The methodological basis of the study was formal and logical, system and structural analysis, ranking, and generalisation, which allowed: identifying current trends and indicators of cybercrime; clarifying the concept and content of operative-search counteraction to fraud on the Internet; conducting a legal analysis of the criminal law norms of the Republic of Kazakhstan and the EU in the field of fraudulent cybercrime;

[*]Doctoral Student. Faculty of Postgraduate Education, M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan. Address: Utepov Str., 29, Almaty, Republic of Kazakhstan, 050060. E-mail: sshaisultanov@gmail.com.

[**]Full Doctor in Law, Researcher. Research Center, M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan. Address: Utepov Str., 29, Almaty, Republic of Kazakhstan, 050060. E-mail: talgat.akimzhanov@outlook.com.

[***]Full Doctor in Law, Professor. Department of Criminal Law Disciplines and Law Enforcement, Eurasian Law Academy named after D.A. Kunayev. Address: Kurmangazy Str., 107, Almaty, Republic of Kazakhstan, 050022. E-mail: borisabdrakhmanov@proton.me.

[****]Senior Lecturer. Faculty No. 1 of Training of the Management Staff of the Department of Internal Affairs, M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan. Address: Utepov Str., 29, Almaty, Republic of Kazakhstan, 050060. E-mail: ardakbazarlinova@hotmail.com.

[*****]Senior Lecturer. "Aikis Travel" Company. Address: Kydyrov Str., 39A, Almaty, Republic of Kazakhstan, 050006. E-mail: A.Bazarlinova@protonmail.com.

investigating the processes for identifying and preventing fraudulent cybercrimes by law enforcement institutions; highlighting certain aspects of protection against Internet fraud; analysing individual criminological strategies for preventing fraudulent crime using the Internet; identifying the features of interaction between government agencies in the field under study; considering key problematic issues of preventing fraudulent offences on the Internet and ways to solve them; revealing the prospects for the development of methods to combat fraudulent cybercrimes.

[Findings] The main results of the study were the definition of modern approaches to the interpretation of the concepts of "cybercrime," "fraud," "operative-search counteraction"; consideration of the regulatory support of Kazakhstan and the member states of the EU in the field of combating Internet fraud; clarification of the issue of criminal identification of fraudulent cybercrimes; clarification of practical aspects of operative-search measures to counteract fraudulent offences on the Internet; generalisation of possibilities for improving operative-search counteraction to fraud committed via the Internet. The significance of the results lies in the provision of practical recommendations regarding the concept and methods of operative-search counteraction to Internet fraud.

Keywords: Cyberspace. Cybercrime. Crimes against property. Procedural actions. Crime prevention.

INTRODUCTION

Cybersecurity is increasingly regarded as one of the fundamental problems of most countries in modern conditions, with regard to its security and the sphere of public life. Meanwhile, fraud is becoming widespread as a way of illegally seizing someone else's property. At the same time, due to the profitability and availability of information technologies, the latter began to be used in the activities of criminals and criminal structures. Because of the fraud on the Internet, citizens of each state will suffer significant damage.

A significant increase in cases of property cybercrime implies the need for a systematic analysis of the prerequisites for the occurrence of relevant offences and the possibilities of preventing and combating them. Attempts by some states, in particular Kazakhstan, to establish criminal liability for Internet fraud at the national level do not solve the general problem of cybercrime since, as practice shows, it seems easy for criminals to circumvent the relevant national restrictions (SHOPINA et al., 2019; ORLOVSKYI et al., 2022). That is why countering fraudulent cybercrimes requires serious efforts not only by individual countries but also by international institutions. Thus, the purpose of the study was a comprehensive analysis of the essence, legal grounds, types, and features of methods of combating Internet fraud and determining the prospects for improving the legislative and practical aspects of identification and operative-search measures to counter fraudulent cybercrime.

D. Neogi (2021), analysing the issues of countering cybercrime, pointed out that the limitless cyberspace provided its users with ample legal and illegal opportunities, so law enforcement agencies are faced with a new type of offence that causes damage at the local and transnational levels. In the meantime, some types of cybercrime are replaced by others every year. J. Koziarski and J.R. Lee (2020), studying the methods of policing in the field of cybercrime, noted that if the response measures of law enforcement agencies to cybercrime are not improved, this may negatively affect their institutional legitimacy as effective state bodies. After all, legislative procedures and the process of investigating crimes are mostly formalised and take considerable time.

Exploring ways to train in the fight against Internet fraud, W. Fang et al. (2021) pointed out that the number of fraud methods on the Internet is constantly increasing along with the rapid development of Internet financial models and Internet business, which leads to unprecedented risks of online fraud. In this case, the victims of this type of crime can be both individuals and companies, or enterprises. In turn, G. Li and Y. Wen (2022), considering measures to counteract the detection of fraud in telecommunications networks, noted that fraud on the Internet exists because of the fact that it can be carried out without the risk of personal contact, which allows criminals to receive illegal income. In particular, there are ways to conceal the location of an individual who is an Internet user and her personal data (JATKIEWICZ, 2023).

Z. Alkhalil et al. (2021), studying phishing attacks as a type of Internet fraud, proved that in the case of international Internet crimes, even if the identity of the offender is found out, differences in the relevant national legislation make it almost impossible to bring such a criminal to justice. According to B.M.S. Al-Khafagy (2020), analysing international measures to combat cybercrime, as criminals continue to improve the technique of committing Internet fraud, the mechanisms for investigating such crimes will always lag behind the development of cybercrime, and the level of solving Internet fraud will remain low.

Consequently, the absence of proper regulatory and legal consolidation of types of cybercrimes, operative-search mechanisms to counter fraudulent Internet crimes, and strategies for the development of methods to combat fraud on the Internet can lead to an increase in the scale of offences on the Internet, which indicates the need for additional research in the relevant field.

MATERIALS AND METHODS

The defining role in the study was played by the formal and logical method, which identified the features of individual legal phenomena and their legal nature. Using the formal and logical method, it was possible to investigate the genesis of the development of crime on the Internet, current trends, and indicators of

cybercrime. In particular, the study established the legal nature and content of the concepts of "cybercrime," "fraud," "operative-search counteraction." Approaches to the interpretation of measures to counteract Internet fraud are summarised. The features of the regulatory support of Kazakhstan and the EU member states in the field of combating Internet fraud are characterised. Based on the system and structural analysis, it was possible to establish structural connections between variables or elements of the system under study.

System and structural analysis allowed conducting a legal analysis of the criminal law norms of the Republic of Kazakhstan and the EU in the field of fraudulent cybercrimes; investigating the processes of detection and prevention of fraudulent cybercrimes by law enforcement institutions; highlighting certain aspects of protection against Internet fraud; analysing individual criminological strategies for preventing fraudulent crime using the Internet; identifying the features of interaction between government agencies in the field under study. The powers of international organisations and institutions in the field of countering Internet fraud are also defined. The issues of interstate interaction between law enforcement agencies in the field of countering fraud committed on the Internet are investigated. Based on the ranking method, which allowed quantifying and distinguishing crime rates, indicators of the number of Internet frauds committed in Kazakhstan and the world during 2019-2022, as well as the amount of damage caused by offences related to fraud on the Internet, were established. By means of the generalisation method, the general features and properties of a certain class of objects are consolidated, and the transition from the singular to the general, from the less general to the more general, is carried out.

Using the generalisation method, it was possible to identify the key problematic issues of preventing fraudulent offences on the Internet and ways to solve them, as well as the prospects for the development of methods to combat fraudulent cybercrimes. The analysis of the issue of criminal identification of fraudulent cybercrimes is carried out. The factors contributing to the development of Internet fraud have been identified. A number of open data sets on the volume and number of fraudulent offences committed on the Internet were also analysed; their main types were identified. The practical aspects of operative-search measures to counteract fraudulent offences on the Internet were determined. The practical challenges and limitations of current measures to prevent and combat fraudulent cybercrimes on the Internet were examined. The possibilities of improving operative-search counteraction to fraud committed via the Internet are considered.

The theoretical basis of the study is papers by researchers and practitioners from Kazakhstan, the countries of the European Union, the United States of America in the field of cybercrime related to fraud, within the limits of the need

to investigate the issue of operative-search counteraction to Internet fraud. The normative basis of the study is the current and prospective legislation in the field of operative-search fight against Internet fraud, including the Law of the Republic of Kazakhstan "On Informatisation" (2015), the Criminal Code of the Republic of Kazakhstan (2023), the European Convention on Human Rights (1950), the Charter of Fundamental Rights of the European Union (2000), the Budapest Convention on Crime in Cyberspace (2001), Directive (EU) 2017/1371 of the European Parliament and of the Council (2017), Directive 95/46/EC of the European Parliament and of the Council (1995), and other legal positions of judicial practice. Each of the issues under study is analysed separately. The study provides general recommendations for improving the understanding and counteraction mechanisms of law enforcement agencies in relation to fraudulent offences committed on the Internet.

RESULTS

The Nature and Types of Fraud Using the Internet

The term "economic crimes" without a single definition is becoming increasingly used in modern society and covers such concepts as fraud, corruption, money laundering, crimes against intellectual property, and individual cybercrimes. Fraud refers to a wide range of criminal behaviour where a person provides false information in order to gain benefit for themselves or third parties, to harm such persons, or to expose them to a risk of loss (BUTTON, 2021; SALIU et al., 2022). The main factors that are prerequisites for the commission of Internet scams are the deepening of society into the virtual environment and psychological reasons. After all, victims of fraudulent schemes, as a rule, are persons who are not well-informed in Internet technologies or who have fallen under the influence of criminals. Meanwhile, the concept of cybercrime originally appeared in America, and later in another world in the early 1960s and included violations of the rights and interests of others using automated information processing systems.

One example of a cybercriminal of that time was John Draper, who was arrested in the 1970s for counterfeiting telephone devices. In the 1980s, Ian Murphy managed to hack into AT&T's communications system, which negatively affected the quality of telephone services. Robert Morris created the first computer worm in 1988. In 1991, computer viruses ("Melissa" and "I LOVE YOU") led to numerous failures of email systems (BAYDALA, 2020). In the 2000s, cyberattacks by criminals gained momentum and became more purposeful. In the meantime, in the 21st century, scammers began to use the Internet in order to obtain monetary and political advantages.

Today, cybercrime involves offences committed in the information and telecommunications sphere, targeting information, tools, and equipment as targets

and instruments of offense (JATKIEWICZ, 2013). The growth of cybercrime indicators is due to the constant improvement of information technologies, the imperfection of legislation in the relevant field of relations, the unpreparedness of law enforcement officers, the lack of technical means and technologies for fixing Internet offences, and conducting appropriate examinations (METELSKYI and KRAVCHUK, 2023). Cases of international cybercrime are also becoming more widespread. Among such Internet offences are those that are related to data theft or modification, computer networks, hacking and virus distribution, and computer fraud and computer forgery (SWIATKOWSKA, 2020).

Meanwhile, fraud using the Internet is also divided into several subspecies: carding (fraudulent transactions with bank cards, card details); vishing (misuse of IP telephony, voice change software, text messages, and social engineering), sniffering (data interception), phishing (misleading owners e-mail addresses) (REZNIK et al., 2021; KIPANE et al., 2023). The increased risks of using the Internet do not mean the need to slow down the development of new technologies or modern ways of using existing technologies, since they are rapidly developing. In particular, this concerns artificial intelligence (WALKER, 2019).

Nevertheless, Internet scams cause enormous losses not only to citizens around the world but also to states as a whole. Thus, the highest damage rates are observed in Europe and Central Asia, North America, and East Asia. Most of the countries in these regions are high-yield countries. It is in these states that cyber risk indices are much higher, which is conditioned by, in particular, a more developed technological infrastructure and a high level of urbanisation and digitalisation of business structures and government (SVIATUN et al., 2021). In the European Union, the largest losses are Internet fraud related to money laundering in its various manifestations, namely: carousel fraud (represented in Germany and Belgium), fraud with social benefits and investments (in Austria), online fraud (Cyprus and Sweden), fraud with social engineering and virtual currencies (Lithuania) (COTOC et al., 2021). These cybercrimes are also accompanied by tax crimes, corruption, drug and human trafficking, organised crime, gambling, and investments. According to forecasts, in 2023, the annual global damage from cybercrime will reach USD 8 trillion. In total, in the next five years, it is expected that the costs of cybercrime will increase by 15% and reach USD 10.5 trillion by 2025 (NIVEDITA, 2023). The extent of damage caused by fraud on the Internet worldwide from 2020 to 2022 is shown in Table 1.

Year	Amount of Material Damage (in USD)
2020	17.5 billion
2021	20 billion
2022	41 billion

Table 1 – Amount of Damage Caused by Internet Fraud in the World (2020-2022)
Source: J. Nivedita (2023).

As for Kazakhstan, trends in Internet fraud are presented in Table 2.

2020	2021	2022
14155 crimes	21405 crimes	20500 crimes

Table 2 – Quantitative Indicators of Fraudulent Internet Crimes in Kazakhstan (2020-2022)
Source: D. Terlikbaev (2022), D. Kaliakparov (2023).

Thus, it is possible to observe an increase in the number of cases of Internet fraud in Kazakhstan, which necessitates the development of legislation to combat cybercrime and the creation of special training courses for specialists in the police, prosecutor's office, judicial authorities, and expert institutions.

Legal Grounds and Mechanisms for Combating Fraudulent Cybercrimes

The concept of "counteraction" is often used in relation to different spheres of activity: offenders in relation to the investigation procedure; society in relation to crime; law enforcement agencies in relation to certain types of crime. The immediate tasks of the employees of the operative-search units of law enforcement agencies are to search and record the actual circumstances in relation to criminal offences, as well as the organisation and conduct of the pre-trial investigation process. The state takes a number of measures to counteract crime in general, including detection, fixation, investigation of criminal offences; prevention of offences, assistance in compensation for harm, and cooperation with public institutions (SAMOILENKO and TITUNINA, 2021). Therefore, counteraction presupposes a system of measures and methods of activity for state and non-state bodies. Therefore, the development of a sound methodology for countering fraud committed on the Internet will be able to characterise the current state of the development of illegal behaviour on the Internet.

The legal basis for countering fraud committed on the Internet presupposes the existence of sufficient national legislation and the harmonisation of relevant practices in combating cybercrime at the regional and international level (SVIATUN et al., 2021). Legal sufficiency here should be assessed based on the number of legal institutions and restrictions related to cybersecurity and cybercrime. In the meantime, the difference in legislation due to the diversity of its jurisdiction may lead to a conflict of jurisdiction between states on international Internet fraud (MPHATHENI and MALULEKE, 2022). After all, cybercrime can be committed on the territory of one country, and the criminal is

located on the territory of another. The Law of the Republic of Kazakhstan "On Informatisation" (2015) established that the protection of informatisation is carried out in relation to: electronic information systems (their owners and users); objects of information and communication infrastructure (their owners).

For the first time, responsibility for cybercrime in Kazakhstan was established by the Criminal Code of the Republic of Kazakhstan in 1997. Article 227 of the Code provided for criminal liability for "illegal access to computer information, creation, use, and distribution of malicious computer programs" with subsequent amendments (LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 154-XIII…, 1994). The modern Criminal Code of Kazakhstan includes nine articles establishing responsibility for crimes in the field of computer information. In addition, 15 additional offences were introduced into the Code, which can be committed using information and communication networks (CRIMINAL CODE OF THE…, 2023).

The specific feature of fraud committed against Internet users is that the latter is recognised as completed from the moment when the victim was transferred to the criminal (their accomplices) money or personal data (REGULATORY RESOLUTION OF THE…, 1998). In turn, EU legislation also protects Internet users from fraud, the essence of which is disclosed in Article 190, part 2, paragraph 4 of the Criminal Code of the Republic of Kazakhstan (2023). In order to combat crime in cyberspace, the Budapest Convention on Crime in Cyberspace (2001) was adopted within the EU, which became the foundation for the development of legislation in the fight against cybercrime at different levels of the territorial organisation of power. This Convention provides for the idea of international cooperation and solidarity in the fight against cybercrime and has been ratified by 18 states and signed by 25 countries. In addition, the protection of privacy is a key policy objective of the Council of Europe and the European Union. The right to confidentiality is consolidated in Article 8 of the European Convention on Human Rights (1950), Articles 7, 8 of the Charter of Fundamental Rights of the European Union (2000), and Directive 95/46/EC of the European Parliament and of the Council (1995).

The European Agency for Network and Information Security regularly conducts educational and public educational campaigns aimed at Internet users, thereby contributing to the safer behaviour of people on the Internet and their digital literacy (REGULATION (EU) 2019/881 OF..., 2019). The powers to counter Internet fraud are assigned to the divisions of the European Anti-Fraud Department and Europol. As for the European Anti-Fraud Department (OLAF), its competence includes:

- Investigation of fraud and other illegal activities;

- Identification and investigation of serious violations by EU employees related to fraudulent activities;
- Assisting the European Commission in formulating and implementing a fraud prevention and detection policy.

The European Cybercrime Centre was created to strengthen the response of law enforcement agencies to fraud on the Internet. Its purpose is to provide the EU police with a central platform for coordinating investigations and collecting information on cybercrime activities. The EU is also discussing Directive (EU) 2017/1371 of the European Parliament and of the Council (2017), with the help of which a legal framework will be created for the functioning of the European Prosecutor's Office, which will be able to consider issues related to Internet fraud. Interpol is an observer organisation of the Budapest Convention on Crime in Cyberspace (2001). It also promotes research, capacity development, and cooperation between EU member states in the fight against cybercrime and financial crimes. The United States of America is the country with the largest number of offenders and victims in terms of cyberattacks and cybercrime. In the United States, there are Internet fraud investigation agencies, task forces, and legally established partnerships between federal agencies fighting cybercrime. For example, the Federal Bureau of Investigation is the main agency investigating cyberattacks by state and non-state organisations (GUNDUR et al., 2021; ADANBEKOVA et al., 2022).

The rapid growth of cybercrime requires the development of effective mechanisms to prevent such crimes. However, the identification and prosecution of cybercriminals is quite rare in accordance with the number of such offences. The development of the strategy of state mechanisms to combat Internet fraud should be aimed at modernising information systems to reduce the scale of cybercrime and create basic principles of national and international policy in the relevant area (SVIATUN et al., 2021). In the process of legal regulation of operative-search counteraction to fraud committed via the Internet, there are the following problematic aspects (KRYSHEVYCH et al., 2021):

1) There is no proper normative distinction between crimes committed on the Internet and offences committed via the Internet.
2) There are no criteria for determining the jurisdiction of criminal proceedings based on the facts of Internet fraud.
3) The possibility of "monitoring the Internet" is not provided.
4) There are no powers to combat cybercrime among the powers of law enforcement agencies.

Another problem is the lack of adequate resources to search for cybercriminals and the preservation of evidence of relevant offences. Training Internet users reduces their vulnerability to Internet fraud, which prevents an increase in the level of victimisation (ALKHALIL et al., 2021). The main areas of countering fraud on the Internet should also include: ensuring the presence of law enforcement agencies in a virtual environment; conducting targeted campaigns, lectures, and consultations among law enforcement officials on the prevention of cybercrime. Work on the prevention of Internet fraud among Internet services, banking and other payment systems, social networks; publication of official analytical reviews and statistical data on the identification of facts of cybercrime; holding events on cybersecurity (SAMOILENKO and TITUNINA, 2021; KERIMKHULLE et al., 2023). It is also important to ensure the procedural interaction of law enforcement agencies during the investigation of Internet fraud, which includes: execution of orders for conducting investigative actions; providing access to materials collected in the course of operative-search activities; assistance in conducting individual investigative actions; and verification of important information (CHUCHKO, 2020). This may also include international legal cooperation, which includes the following activities: information exchange, transfer of investigative procedures, and extradition (MPHATHENI and MALULEKE, 2022).

DISCUSSION

The analysis of literature sources allows for asserting the absence of comprehensive special studies devoted to the problem of operative-search counteraction to fraud committed via the Internet. To date, the provisions regarding the partial regulation of the legal nature of countering fraudulent cybercrime and the specifics of its understanding and implementation are consolidated in the Law of the Republic of Kazakhstan "On Informatisation" (2015), the Criminal Code of the Republic of Kazakhstan (2023), the European Convention on Human Rights (1950), the Charter of Fundamental Rights of the European Union (2000), the Budapest Convention on Crime in Cyberspace (2001), Directive (EU) 2017/1371 of the European Parliament and of the Council (2017), Directive 95/46/EC of the European Parliament and of the Council (1995), and other legal positions of judicial practice. Nowadays, because the Internet has become one of the main means of human life, it is not difficult to imagine that offenders and terrorist organisations will use this tool to destabilise society. Hence, any state should be aware of the significance of this problem and take all necessary measures to prevent the occurrence of Internet fraud. This is conditioned by the high level of victimisation and high consumer confidence in the provision of banking services and online shopping.

C. McKoy (2021) noted that the potential of significant Internet threats is dominated by institutional capabilities to combat relevant offences. There is a gap between the need for cybersecurity and the effectiveness of measures regarding it. In turn, the author believes that individual states still manage to successfully resist the emergence of new types of cybercrime, which is primarily related to the economic and social development of the country. T.K. Yerjanov et al. (2017) suggest that modern types of cybercrime include, in particular, cyberterrorism and theft of personal data. It is impossible to fully agree with this opinion because, in fact, the list of cybercrimes is much wider, and some of them have not yet been singled out due to insignificant indicators of the corresponding type of crime. Regarding the definition of cybercrime, T. Van Nguyen et al. (2022) pointed out that there is no single interpretation of such a concept, which leads to the levelling of economic losses that occur as a result of Internet offences worldwide. Since most crimes involving the use of the Internet are related to copyright violations, fraud, the distribution of pornographic materials, and violations of network security.

A. Zingerle and L. Kronman (2018) noted that previously victims in most cases received "unwanted mass emails," and now the widespread use of social networks and messaging applications and a significant increase in the number of malware requesters have opened up opportunities for fraudsters. This is conditioned by the high level of victimisation and the high level of trust in the population. At the same time, the author suggests that today, the forms and methods of fraud on the Internet have been significantly reformatted, since cybercrime has begun to focus in the areas of banking services and online shopping. Over the years, the negative side of the Internet has manifested itself in various forms: unauthorised access, the spread of disinformation through digital communication channels, online fraud, illegal trade, and organised crime.

In turn, A.F. Al-Qahtani and S. Cresci (2022) noted that the COVID-19 pandemic forced many workers to work remotely, using special digital platforms, messaging applications, and new communication channels, resulting in a massive escalation of cyberattacks. During this period, cybercriminals managed to use the personal data and documents (which were uploaded to remote work platforms) of hundreds of thousands of people to satisfy their own property interests.

G. Norris et al. (2019) emphasised that the victim causes of Internet scams should also be considered, that is, psychological factors that contribute to people becoming victims of scams. Supporting this position, in order to combat fraud and cybercrime, it is necessary to provide mechanisms for the protection and training of potential victims of fraud. In particular, this concerns the rules for conducting online transactions, which today are the basis of the e-commerce industry. Therefore, one of the ways to commit fraud on the Internet is to commit criminal

acts with cryptocurrencies, which have become legal means of payment in most countries in the world (VILKS and KIPANE, 2018).

S. Walker (2019) pointed out that the inter-jurisdictional nature of cybercrime makes it necessary to respond to this type of criminal activity, which is quite difficult at the national level. Meanwhile, some states have managed to adopt laws regulating crime on the Internet. It should be noted that one of the most difficult stages of operative-search activity in this context is finding the location of an Internet fraudster, who, with the help of VPN technologies, can constantly change the IP address of electronic devices with which cybercrimes are committed. J. Swiatkowska (2020) identified three key elements of cybersecurity: confidentiality, availability, and storage of data in networks and information systems. In general, cybersecurity implies a state where Internet users can safely act and achieve their goals through effective risk management. However, the author suggests that responsibility for their own cybersecurity should not be placed solely on the users themselves, since, first of all, states should take care of the safety of their citizens in any environment; this also applies to the Internet.

In the context of property crimes W. Werapun et al. (2023) proved that due to the availability of new financial opportunities, many fraudulent methods of using instant loans appeared on the Internet, allowing attackers to manipulate the financial market. In contrast, G. Li and Y. Wen (2022) noted that in the process of combating cybercrime, in order to ensure the legality and effectiveness of the operative-search process, law enforcement agencies should improve their investigative and criminalistic potential. This view must be accepted, as law enforcement agencies are the initial institutions directly involved in detecting and investigating cybercrime.

C.N. Cotoc et al. (2021) suggest that in order to strengthen the effectiveness of countering crimes on the Internet, in particular, with regard to money laundering and terrorist financing, it is necessary to systematically assess the implementation of relevant EU legislation and provide transparent and standardised statistical reports in this area. In the meantime, researchers do not note how such an assessment should be made. The author admits that reports should not be provided by the highest legislative and executive bodies but should be submitted from lower management structures to higher ones. This would allow for the recording of the real scale of the development of Internet fraud and the effectiveness of existing methods of countering this type of fraud.

Among the measures to reduce the risks of potential harm from Internet fraud, which were envisaged by R. Basheer and B. Alkhatib (2021), are avoidance of identity identification, avoidance of disclosure of confidential personal data, taking measures to download malicious files, and avoidance of data leakage. As noted by S. Chuchko (2020), when investigating the cooperation of investigators

and operational staff in the process of exposing fraud on the Internet, the management levels that should be considered are the work of special departments and divisions and the investigation of a specific offence. In contrast, the author suggests that cooperation should take place between law enforcement and judicial authorities at all levels, which would ensure a timely response to every case of cybercrime. In addition, chronic problem law enforcement agencies face in their operative-search activities in connection with Internet fraud is the erroneous establishment of the circle of perpetrators (including from the point of view of evidentiary rules), making it difficult to identify real criminals and investigate relevant offences (SHEVCHUK et al., 2022).

M. Button (2021) believed that Internet fraud creates extraordinary challenges for law enforcement agencies: they are subject to special legislation, according to which most employees do not have in-depth training; there is no clear evidence of committed offences. But in fact, this is not the main problem in countering cybercrime. In particular, other scientific views on the issue under study should be considered. S.Y.K. Wang et al. (2021) pointed out that positive results from countering Internet fraud can be observed in the case of updating the legal system of the state and using active and flexible approaches to cyberspace management.

CONCLUSIONS

As a result of the conducted research, it was determined that cybercrime includes a set of offences committed in the information and telecommunications spheres. Internet scams cause enormous losses not only to citizens around the world but also to states as a whole. Internet fraud is an offence aimed at economic or property losses carried out by misleading people directly using computers and Internet technologies.

It was found out that Internet fraud is divided into several types: carding fraud, vishing, sniffering, and phishing. It was revealed that the counteraction to Internet fraud includes the identification, documentation, investigation, and prevention of relevant offences. It is established that, for the first time, responsibility for cybercrime in Kazakhstan was established by the Criminal Code of the Republic of Kazakhstan. In turn, there are a number of bodies in the EU whose competence, among other things, includes countering Internet fraud, such as the European Anti-Fraud Department, Europol, the European Cybercrime Centre, and Interpol. At the same time, in the United States, there is a Federal Bureau of Investigation for the same purposes, which, in particular, is authorised to identify, investigate, and combat Internet crimes. A number of problems in the field of operative-search counteraction to crimes committed on the Internet have been clarified: improper normative differentiation of crimes committed on the

Internet and offences committed via the Internet; lack of criteria for determining the jurisdiction of criminal proceedings on the facts of Internet fraud; lack of state monitoring of the Internet; lack of legislatively specified powers of law enforcement agencies in the field of combating cybercrime; lack of adequate resources to search for cybercriminals; and preservation of evidence of relevant offences.

The necessity of bringing the existing national laws of the EU states, as well as those of the Republic of Kazakhstan, to the real needs of the operational and investigative activities of law enforcement agencies regarding crimes committed on the Internet is considered. Countering fraud on the Internet should include: training Internet users and law enforcement officials to prevent cybercrime; work to prevent Internet fraud among Internet services, banking and other payment systems, social networks; the publication of reviews and statistics on the identification of facts of cybercrime; the procedural interaction of law enforcement agencies; and international legal cooperation.

The materials of this study can be used in the development of additions and amendments to relevant resolutions, charters, regulations of EU institutions, national legislation of Kazakhstan, state programmes to combat cybercrime, and concepts and strategies of the state. In the course of the research, new issues arose that needed to be addressed. It is necessary to continue the study of the essence, legal grounds, types, and features of methods to combat Internet fraud and identify prospects for improving the legislative and practical aspects of identification and operative-search measures to counter fraudulent cybercrimes, their problems, and solutions.

REFERENCES

ADANBEKOVA, Z. N., OMAROVA, A. B., YERMUKHAMETOVA, S. R., KHUDAIBERDINA, G. A., & TYNYBEKOV, S. T. (2022). Features of the conclusion of a civil transaction on the internet. *International Journal of Electronic Security and Digital Forensics*, *14*(1), 19-36.

AL-KHAFAGY, B. M. S. (2020). International efforts to combat cybercrime. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *17*(6), 3034-3054.

ALKHALIL, Z., HEWAGE, C., NAWAF, L., & KHAN, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

AL-QAHTANI, A. F., & CRESCI, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Information Security*, *16*(5), 324-345.

BASHEER, R., & ALKHATIB, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications*, *2021*, 1302999.

BAYDALA, B. D. (2020). Combating health care cyber crime. *Journal of Healthcare Risk Management*, *40*(2), 15-20.

BUDAPEST CONVENTION ON CRIME IN CYBERSPACE DATED NOVEMBER 23, 2001. (2001). Available at: http://zakon0.rada.gov.ua/laws/show/994_575

BUTTON, M. (2021). Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a National Economic Crime Agency. *Policing: A Journal of Policy and Practice*, *15*(3), 1758-1772.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. (2000). *Official Journal of the European Communities*, *364*, 1-22. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

CHUCHKO, S. (2020). Features of the interaction of law enforcement agencies in the investigation of fraud in the purchase and sale of goods via the Internet. *Entrepreneurship, Economy and Law*, *12*, 267-271.

COTOC, C. N., NITU, M., SCHEAU, M. C., & COZMA, A. C. (2021). Efficiency of money laundering countermeasures: Case studies from European Union member states. *Risks*, *9*(6), 120.

CRIMINAL CODE OF THE REPUBLIC OF KAZAKHSTAN DATED JULY 3, 2014. No. 226-V (as amended and supplemented as of March 26, 2023). (2023). Available at: https://online.zakon.kz/m/amp/document/31575252

DIRECTIVE (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. 2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L1371

DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

EUROPEAN CONVENTION ON HUMAN RIGHTS as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, dated September 3, 1953. (1950). Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf

FANG, W., LI, X., ZHOU, P., YAN, J., JIANG, D., & ZHOU, T. (2021). Deep Learning anti-fraud model for internet loan: Where we are going. *IEEE Access*, *9*, 9777-9784.

GUNDUR, R. V., LEVI, M., TOPALLI, V., OUELLET, M., STOLYAROVA, M., CHANG, L. Y. C., & MEJIA, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context. Available at: https://www.crimrxiv.com/pub/48bmtkg0/release/3

JATKIEWICZ, P. (2023). Security and confidentiality of personal data on the internet. *Journal of the Balkan Tribological Association*, *29*(5), 802-817.

KALIAKPAROV, D. 2023. More than 20 thousand cases of Internet fraud recorded in 2022. Available at: https://total.kz/ru/news/zhizn/bolee_20_tisyach_sluchaev_internetmoshennichestva_zafiksirovano_v_2022_godu_date_2023_01_23_13_30_33

KERIMKHULLE, S., DILDEBAYEVA, Z., TOKHMETOV, A., AMIROVA, A., TUSSUPOV, J., MAKHAZHANOVA, U., ADALBEK, A., TABERKHAN, R., ZAKIROVA, A., & SALYKBAYEVA, A. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry*, *15*(10), 1958.

KIPANE, A., VILKS, A., & KRIVINCH, A. (2023). Forecasts of Long-term Progress in the Socio-cultural Sphere in the Context of Combating Economic Crime. *Pakistan Journal of Criminology*, *15*(4), 49-67.

KOZIARSKI, J., & LEE, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, *43*(1), 198-211.

KRYSHEVYCH, O., ANDRUSHCHENKO, I., STRILTSIV, O., PYVOVAR, Y., & RIVCHACHENKO, O. (2021). Modern methods of computer-related fraud: Legal characteristics and qualification. *Cuestiones Politicas*, *39*(68), 844-865.

LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 154-XIII "On operational-search activity". (1994). Available at: https://adilet.zan.kz/rus/docs/Z940004000_

LAW OF THE REPUBLIC OF KAZAKHSTAN NO. 22-V "On Informatisation". (2015). Available at: https://online.zakon.kz

LI, G., WEN, Y. (2022). Research on the detection countermeasures of telecommunication network fraud based on big data for killing pigs and plates. *Journal of Robotics*, *2022*, 4761230.

MCKOY, C. (2021). Law enforcement officers' perceptions in combating cybercrime at the local level. Walden Dissertations and Doctoral Studies,

11204. Available at: https://scholarworks.waldenu.edu/dissertations/11204

METELSKYI, I., & KRAVCHUK, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, *1*(1), 18-25.

MPHATHENI, M. R., & MALULEKE, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science*, *11*(4), 384-396.

NEOGI, D. (2021). Combating cyber crime: How can technology intervention supplement legal provisioning? *International Journal of Service Science, Management, Engineering, and Technology*, *12*(6), 1-15.

NIVEDITA, J. (2023). 90+ cyber crime statistics 2023: Cost, industries & trends. Available at: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/

NORRIS, G., BROOKES, A., & DOWELL, D. (2019). The psychology of Internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231-245.

ORLOVSKYI, R., Us, O., & SHEVCHUK, V. (2022). Committing a Criminal Offence by an Organized Criminal Group. *Pakistan Journal of Criminology*, *14*(2), 32-45.

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity). (2019). Available at: http://data.europa.eu/eli/reg/2019/881/oj/

REGULATORY RESOLUTION OF THE SUPREME COURT OF THE REPUBLIC OF KAZAKHSTAN NO. 1 "On some issues of application of legislation on the judiciary in the Republic of Kazakhstan". (1998). Available at: https://adilet.zan.kz/rus/docs/P98000001S_

REZNIK, O., FOMENKO, A., MELNYCHENKO, A., PAVLOVA, N., & PROZOROV, A. (2021). Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga, 10*(41), 141-150.

SALIU, H., REXHEPI, Z., SHATRI, S., & KAMBERI, M. (2022). Experiences with and risks of internet use among children in Kosovo. *Journal of Elementary Education*, *15*(2), 145-164.

SAMOILENKO, O., & TITUNINA, K. (2021). Internet fraud: technologies of performance, ways of counteraction and prevention. *ScienceRise: Juridical Science*, *2*(16), 65-70.

SHEVCHUK, V., VAPNIARCHUK, V., BORYSENKO, I., ZATENATSKYI, D., & SEMENOGOV, V. (2022). Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense*, *32*, 320-341.

SHOPINA, I. N., MULIAVKA, D. G., HRECHANIUK, S. K., & FEDCHYSHYNA, V. V. (2019). Improvement of social control as a direction of crime prevention. *Russian journal of criminology*, *13*(3), 447-454.

SVIATUN, O. V., GONCHARUK, O. V., CHERNYSH, R., KUZMENKO, O., & KOZYCH, I. V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762.

SWIATKOWSKA, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. Oxford: Pathways for Prosperity Commission Background Paper Series.

TERLIKBAEV, D. (2022). Is it true that cybercrime in Kazakhstan has increased 10 times in 5 years? Available at: https://factcheck.kz/truth/pravda-li-chto-kiberprestupnost-v-kazaxstane-vyrosla-v-10-raz-za-5-let/

VAN NGUYEN, T., TRUONG, T. V., & LAI, C. K. (2022). Legal challenges to combating cybercrime: An approach from Vietnam. *Crime, Law and Social Change*, *77*, 231-252.

VILKS, A., & KIPANE, A. (2018). Economic crime as a category of criminal research. *Journal of Advanced Research in Law and Economics*, *9*(8), 2860-2867.

WALKER, S. (2019). Cyber-insecurities? A guide to the UN cybercrime debate. Available at: https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf

WANG, S. Y. K., HSIEH M. L., CHANG, C. K. M., JIANG, P. S., & DALLIER D. J. (2021). Collaboration between law enforcement agencies in combating cybercrime: Implications of a Taiwanese case study about ATM hacking. *International Journal of Offender Therapy and Comparative Criminology*, *65*(4), 390-408.

WERAPUN, W., KARODE, T., ARPORNTHIP, T., SUABOOT, J., SANGIAMKUL, E., BOONRAT, P. (2023). The flash loan attack analysis (FAA) framework – A case study of the warp finance exploitation. *Informatics*, *10*(1), 3.

YERJANOV, T. K., BAIMAGAMBETOVA, Z. M., SERALIEVA, A. M., ZHAILAU, Z., & SAIRAMBAEVA, Z. T. (2017). Legal issues related to combating cybercrime: Experience of the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics*, *8*(7), 2276-2291.

ZINGERLE, A., & KRONMAN, L. (2018). Internet crime and anti-fraud activism: A hands-on approach. Hershey: IGI Global.

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