ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.40

Nº 73
Julio
Diciembre
2022

Cuestiones Políticas Vol. 40, Nº 73 (2022), 377-402
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Criminal law and forensic support in the fight against cybercrime

DOI: https://doi.org/10.46398/cuestpol.4073.20

Valentin Kovalenko *
Anatolii Kryzhanovskyi **
Oleksandr Kolb ***
Svitlana Soroka ****
Halyna Popadynets *****

Abstract

The article analyses legislation and scientific work on combating cybercrime based on the use of a set of general and special methods, methodological principles and approaches of legal science. It is concluded that with the introduction of the term "cybercrime" in the criminal law of Ukraine, the use of the term "cybercrime" becomes relevant, which should be understood as a socially dangerous crime in cyberspace, a responsibility that is provided for by the Ukrainian law on criminal responsibility and that is also recognized as a criminal offense by international treaties that regulate the matter. Emphasis is placed on the desirability of making appropriate terminological changes in the Law of Ukraine "On the Basic Principles of Cyber Security" and other regulations, as well as taking other systemic measures at the conceptual and organizational level, to identify the main cybersecurity threats and formulate measures to prevent and investigate them, determine a single body for the operational management of all entities whose task is to ensure the cybersecurity, create a system

* Doctor of Law, Associate Professor, Leading researcher at Copyright and related rights sector of the laboratory of copyright and information technologies of the research center for forensic intellectual property of the ministry of justice of Ukraine, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2041-250X

** Doctor of Law, Senior Lecturer at the Department of Criminal Law and Procedure of the Educational and Scientific Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2432-5286

*** Doctor of Law, Professor, Honored Lawyer of Ukraine, Professor of Criminology and Criminal Enforcement Law at National University of Law Honored Lawyer of Ukraine, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-1792-4739

**** Candidate of Law, Associate Professor, Associate Professor at the Department of Criminal Law and Procedure of the Educational and Scientific Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine. ORCID ID: https://orcid.org/0000-0002-9351-4531

***** Candidate of Philosophical Sciences, Associate Professor, Associate Professor at the Department of Criminal Law and Procedure of the Educational and Scientific Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine. ORCID ID: https://orcid.org/0000-0003-1701-0830

Recibido el 16/03/2022 Aceptado el 28/04/2022

of technological means of the national cybersecurity system and establish closer international cooperation.

Keywords: information space; cybersecurity; cybercrime; criminal liability; classification of crime.

Derecho penal y apoyo forense en la lucha contra el ciberdelito

Resumen

El artículo analiza la legislación y los trabajos científicos sobre la lucha contra el delito cibernético sobre la base del uso de un conjunto de métodos generales y especiales, principios metodológicos y enfoques de la ciencia jurídica. Se concluye que con la introducción del término "delito cibernético" en la ley penal de Ucrania, cobra relevancia el uso del término "delito cibernético", el cual debe entenderse como un delito socialmente peligroso en el ciberespacio, responsabilidad que está previsto por la ley de Ucrania sobre responsabilidad penal y que además está reconocido como un delito penal por los tratados internacionales que regulan la materia. Se hace hincapié en la conveniencia de realizar los cambios terminológicos apropiados en la Ley de Ucrania «Sobre los principios básicos de la seguridad cibernética» y otras regulaciones, así como tomar otras medidas sistémicas a nivel conceptual y organizacional, para identificar las principales amenazas de seguridad cibernética y formular medidas para prevenirlas e investigarlas, determinar un órgano único para la gestión operativa de todas las entidades cuya tarea es velar por la ciberseguridad, crear un sistema de medios tecnológicos del sistema nacional de ciberseguridad y establecer una cooperación internacional más estrecha.

Palabras clave: espacio de información; ciberseguridad; ciberdelincuencia; responsabilidad penal; calificación de delito.

Introduction

The global computerization of modern society affects all spheres of human life and the economy, data transmission via the Internet, electronic signatures, key certification, electronic transactions and payments have become the object of illegal actions. This gives grounds to claim that «cybercrime» in the XXI century will be one of the most numerous. In this regard, the issue of cybersecurity of the state and society as a whole is relevant.

In Ukraine, information security is one of the most important functions of the state, because the welfare of the nation depends on the information component. Due to socio-economic problems, Ukraine lags significantly behind the countries party to the Convention on Cybercrime. Cyber wars, cyber terrorism, cyber espionage have become commonplace, so crime in the information sphere is a significant threat to national security in the economy.

The degree of latency of cybercrime remains, which is due to industrial cyber espionage, and the most common types of such crimes are carding, phishing, vishing, skimming, shimming, online fraud and others.

The registered array of criminal encroachments in the analyzed area indicates a significant increase in the level of these crimes in recent years and has the following indicators: in 2015 were recorded 598 crimes, in 2016 – 865, in 2017 – 2573, in 2018 – 2301, in 2019 year – 2284, in 2020 – 2701 crimes (Uniform report on criminal offenses by state).

There is no doubt that today the criminogenic situation requires the development and implementation of measures to prevent criminal encroachments on facilities in the use of computers, systems, computer networks and telecommunications networks. Despite the fact that the Parliament of Ukraine has tried to regulate the relations arising in cyberspace, namely adopted the Law of Ukraine «On Basic Principles of Cyber Security in Ukraine», the state is constantly a victim of cyber attacks, in connection with which the issue of combating cybercrime, proper criminal law and forensic support in the fight against these crimes becomes especially relevant.

1. Methodology of the study

For the achievement of the most reliable scientific results, the methodological basis for the development of methods and methods of scientific knowledge, the storage of such a systematic approach to the consideration of vivid problems in the modern social world. In the process of a scientific joke, scientific and special methods, methodological principles and approaches to legal science were victorious. The basis of the preliminaries is the dialectical method, which is the scientific method of developing social and legal manifestations in these conflicts, development and changes, which gave the opportunity to value the specialness of the critical legal situation. Logic-semantic method of vikoristano for a thorough understanding of the understanding of the legal qualifications of cyberzlochin and preliminaries of basic fig.

The historical-legal method made it possible to see the genesis of the science of thought and to understand the victors of the legal age. The systemic-structural method allows for the significant number of nutritional problems, such as the quality of the quality and the implementation of state policy in the sphere of fighting against this type of evil. The statistical method is used in the process of public relations, grouping and analysis of empirical material and estimates of the most important indicators of the current cyber-problem in Ukraine and society.

The obstinacy of the comparative (comparative) method has given the opportunity to see through the foreign lands near the struggle with the common malignancies. Synergetic method that allows to develop the composition of criminal law characteristics of cybersecurity, as well as the importance of criminal law and forensic mechanisms to combat cybercrime, which is visualized in the structures of scientific knowledge.

2. Analysis of recent research

The issue of legal regulation of activities in the field of combating crime is a constant subject of scientific research of criminologists. This is largely due to the fact that the development of society and relations in it are permanent processes. As a result, crime as a form of social practice is constantly improving, acquiring new forms and manifestations. Therefore, society and the state are trying to respond accordingly to these processes of «improvement» and «self-improvement» of crime. One of the forms of such a response is law-making – the creation, amendment or repeal of regulations governing the fight against crime. Their purpose is to regulate various legal ways of social relations in the most vulnerable spheres of social life.

Criminal law policy, as a system-forming element of crime policy, which, in turn, is an integral part of all public policy, solves its narrower tasks aimed at creating an effective mechanism for protecting key public relations, values, benefits and interests and combating crime. criminal remedies in terms of sustainable development of the state (Kozych, 2020).

Today, cyber attacks harm not only individuals and legal entities, but also states. Every year, hundreds of events are held around the world to discuss current cybersecurity issues. New definitions are constantly appearing in literary dictionaries: cyber intelligence, cyber terrorism, cyber espionage, cyberspace, critical infrastructure, and so on. Cybersecurity and the fight against cybercrime in the 21st century are among the most important issues that require in-depth analysis, development and implementation of high-tech solutions to prevent and detect cyber threats.

The issue of developing effective legal mechanisms for the international fight against cybercrime has been reflected in the works of many scholars. Among them, in particular: A. Savchenko (Savchenko, 2001), M. Karchevsky (Karchevsky, 2017), E. Skulish (Skulish, 2014), T. Sozansky (Sozansky, 2009), M. Gutsalyuk (Gutsalyuk, 2019), M. Shemchuk (Shemchuk, 2018), D. Richka (Richka, 2019), I. Kozych (Kozych, 2020), A. Sakovsky and M. Klymchuk (Sakovsky and Klymchuk, 2019), O. Samoylenko (Samoylenko, 2020) and others.

At the same time, despite the importance of these and other scientific developments, today there are many problems in the implementation of criminal law policy to combat crime in the use of computers (computer), systems and computer networks and telecommunications networks. In particular, there is no comprehensive criminal-legal analysis of the qualification of crimes in this area, the issues of criminal-legal means of combating cybercrime remain unresolved.

At the same time, the issues concerning the procedural capabilities of the operational units of the National Police of Ukraine and other law enforcement agencies in documenting the illegal behavior of persons who have committed cybercrimes remain insufficiently researched. Within the framework of reforming criminal procedural and operational-search legislation, the problems of detailing legislation that would reflect the provisions of the Convention on Cybercrime on obtaining electronic evidence, restricting (blocking) certain information resources (information services), specific conditions for searching and retrieving digital (electronic) evidence.

The above indicates the relevance and timeliness of the chosen topic of the scientific article.

The purpose of the article is to determine the legal nature of cybercrime, the peculiarities of the regulation of legal provisions on this category of crimes. On this basis, it is important to identify the root causes and forms of cybercrime, to develop appropriate ways to combat the criminal law and forensic level.

3. Results and discussion

3.1. International policy to influence cybercrime

From the point of view of the fundamental legal doctrine – cybercrime consists of criminal acts committed with the help of electronic information and communication means. In other words, cybercrime can be any traditional offline crime (such as theft, fraud, money laundering), but

committed on the Internet. Some researchers also single out «hybrid» or «cyber-driven» crimes and cyber-dependent crimes, which have only been made possible by the development of the Internet and related digital technologies.

A number of countries have developed special laws aimed at combating cybercrime. For example, Germany, Japan and China have amended the relevant provisions of their criminal codes to describe and combat cybercrime. Some countries, instead of dividing cybercrime into separate criminal acts, have simply added specific clauses to their national legislation and codes to criminalize the illicit use of digital technology to commit any crime. This approach has resulted in the offender being charged with two crimes at the same time (Cybercrime, Legal Regulation).

Thus, cybercrime as a phenomenon arose solely in the evolution of computer and information technology, and the purpose of criminals is personal and corporate data, which in themselves are valuable or through which criminals can illegally seize money, intangible assets or property or non-property rights etc. Today, there are many types of cybercrime, among which the biggest threats are: online fraud, DoSattacks, interface, malware (viruses), carding, phishing, computer espionage, online extremism (which is increasingly classified as cyberterrorism), personal insult or slander, etc.

Most of the crimes listed above are committed not only in the territory or in the virtual space of one particular country, they can also be of a more global interstate or even international nature. In fact, this creates a need for international cooperation, as one of the main problems faced by law enforcement operatives in the investigation of cybercrime is the difficulty in establishing the identity of the offender, his state and territorial location, as well as the rule of law under which the offender can be prosecuted.

The active fight against cybercrime is carried out in the countries of the European Union, where the necessary legal framework for the protection of cyberspace has been created. The European Union's cybersecurity strategy was adopted in 2013. Its peculiarity is that the strategy covered various aspects of cyberspace, in particular, the internal market, justice, domestic and foreign policy. Together with the Strategy, a legislative proposal on strengthening the security of the European Union's information systems was developed and adopted, and the priorities of the European Union's international policy in cyberspace, as defined by the Strategy (EU International Cyberspace Policy), were identified.

At present, only 10 of the 27 countries of the European Union have developed national cybersecurity strategies. Today, the most protected countries are Denmark, Great Britain, Finland, Sweden, France and the Netherlands (EU International Cyberspace Policy).

It should be noted that the terms “cybercrime” and “computer crime” are often used interchangeably. However, it is the term cybercrime that best reflects the essence of this phenomenon.

The Law of Ukraine “On the Basic Principles of Ensuring Cyber Security of Ukraine” defines cybercrime as a set of cybercrimes. And cybercrime (computer crime) – as a socially dangerous crime in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine (The Law Of Ukraine “On The Basic Principles Of Ensuring Cyber Security Of Ukraine”, 2017). Thus, today in the legislation of Ukraine there is no clear definition of the concept of “cybercrime”.

The European Convention on Cybercrime outlines a range of socially dangerous acts that may fall under the concept of «cybercrime» at the national level, including illegal access to a computer system, illegal data interception, intrusion into the system, device abuse, forgery and fraud, related to computers; offenses related to child pornography; infringements related to copyright and related rights.

Characteristic features of these crimes are the following: the need for widespread use of special knowledge in the detection and recording of traces of crime in electronic form; organization and transnational character, as national borders are not an obstacle to this phenomenon; information stored in computer systems is short-term; the ability to destroy or alter computer information; detection, recording and retrieval of evidence is a complex process; high level of technical support of offenders; high degree of anonymity; high latency due to the reluctance of victims to inform about such crimes due to distrust in the potential of law enforcement agencies; lack of sustainability of cybercrime due to the constant improvement of computer technology.

It is worth noting that the Council of Europe Convention on Cybercrime is the only binding international instrument in the field of combating cybercrime (Cyber Crime Convention, 2001). It contains a set of basic principles for any country, develops national legislation to combat cybercrime. However, the classification given in the Convention, according to some Western and domestic researchers, is not comprehensive. Initially, the Convention cybercrime was divided into four groups.

Then, in early 2002, a protocol was adopted in addition to the Convention, which supplemented the list of crimes by disseminating racist and other information that incited violence, hatred or discrimination against an individual or group of persons based on racial, religious or ethnic origin. With the development of scientific and technological potential and public relations in cyberspace, this list will, unfortunately, expand. In addition, the crimes listed in the Convention are related to some, but not all, actions that encroach on public safety.

In the report of the Home Affairs Committee of the British Parliament on cybercrime in 2013, cybercrime is divided into three categories:

- exclusively cybercrime, where digital systems are the main target, are also a means of encroachment. This category includes assault on computer systems to destroy the infrastructure of Internet technologies and illegal possession of data;
- existing crimes that have been translated into cybercrime due to the use of the Internet;
- use of the Internet for drug trafficking and as an auxiliary tool for other crimes (Home Affairs Committee E-Crime Fifth Report Of Session, 2013–2014).
- The joint communication of the European Commission in 2013 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions also reveals cybercrime through three main categories:
- traditional types of crimes (for example, fraud, forgery of documents, etc.) committed with the use of electronic communication networks and information systems;
- placement of illegal content in electronic media;
- attacks on information systems, blocking of software of sites and hacking (Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and The Committee Of The Regions, 2013).

Most researchers studying the problem of cybercrime suggest dividing cybercrime into types depending on the object and subject of the attack. The most common divisions as an option are computer crimes and crimes committed with the help of computers, computer networks and other devices to access cyberspace. This position is supported by the fact that the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, which considered measures to combat computer-related crime, considered the concept of cybercrime from two perspectives: cybercrime in the "broad" and "narrow" sense.

Cybercrime in the narrow sense (computer crime): any illegal act committed through electronic operations, the purpose of which is the security of computer systems and the data they process. Cybercrime in the broadest sense (as a computer-related crime): any wrongful act committed with the help of computers or involving computers, computer systems or networks, including the illegal possession and supply or dissemination of information through computer systems or networks.

However, the report of the same Congress states that the term "computer crime" was developed to cover both completely new forms of crime targeting computers, networks and their users, and more traditional crimes that are currently committed using or using computer equipment (Tenth United Nations Congress for Crime Prevention and Treatment, 2000).

In addition, the UN Secretary-General's statement "Findings of a study on effective measures to prevent and combat high-tech and cybercrime" uses the term "traditional crime": "The use of new technologies for criminal purposes has led to completely new forms of crime. On the other hand, more traditional crimes are now being committed by new methods that increase the benefits or reduce the risks for criminals (UN Economic and Social Council. Commission For the Prevention of Crime and Crime, 2001).

Foreign scholars, such as Dr. Mike McGuire and Samantha Dowling (England), also believe that cybercrime is a general term used to describe two different but closely related crimes: cyberdependent and cybercrime (cybercrime).

Crimes committed with the use of computers, computer networks or other forms of communication and information technology. Such as spreading viruses and other malware, DDoS attacks, hacking servers to capture network infrastructure or web pages. Such crimes are aimed at damaging computers and network sources.

Cybercrime is a traditional crime that is exacerbated or achieved through computers, computer networks, or other information and communication technologies. They can still be done without the use of information and communication technologies (McGuire and Dowling, 2013).

It can be argued that doctrinal approaches to understanding the concept of cybercrime are different. However, it is worth noting that despite the available alternative definitions, it is the term cybercrime that best reflects the essence of this phenomenon.

According to the classification of cybercrime, it can be concluded that most researchers studying the problem of cybercrime suggest dividing cybercrime into types depending on the object and subject of encroachment: new crimes made possible by the latest computer technology (crimes under Chapter XVI of the Criminal Code of Ukraine); traditional crimes committed with the help of computer technology and the Internet.Legislation on cybercrime, the development of modern mechanisms for identifying and identifying the perpetrators of cyberattacks and the responsibility for the offense should play an important role in preventing an increase in the number of cyberattacks at the national level.

In a global sense, cybersecurity is the implementation of measures to protect networks, software products and systems from digital attacks.

3.2. National mechanisms for combating cybercrime in Ukraine

In Ukraine, at the legislative level, relevant laws and regulations are adopted that regulate relations in this area. As of the end of 2020, the legal basis of cyber security of Ukraine includes the following regulations: the Constitution of Ukraine, the Criminal Code of Ukraine, the laws of Ukraine «On the basic principles of cyber security of Ukraine», «On information», «On information protection in information and telecommunications systems»,»On the Fundamentals of National Security» and other laws, the Doctrine of Information Security of Ukraine, the Council of Europe Convention on Cybercrime and other international treaties, the binding nature of which was approved by the Verkhovna Rada of Ukraine.

To effectively combat cybercrime in Ukraine, following the example of foreign countries, it would be necessary to: create a political basis (conceptual level), improve the system of legislation (legislative level), identify a system of bodies whose main functions would be cyber defense of Ukraine (institutional level). One of the first steps towards creating a political basis was the adoption of the Presidential Decree «On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the CyberSecurity Strategy of Ukraine».

The main purpose of this Strategy is to ensure safe conditions for the use of cyberspace, protection of the interests of the individual, society and the state. Taking into account all the positive and negative sides of the Strategy, Ukraine must create a large high-tech system to ensure the reliability and security of communications in the information sphere (On The Cyber Security Strategy Of Ukraine, 2016).

Adopted on October 5, 2017, the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» defines the legal and organizational framework for protecting the vital interests of man and citizen, society and the state, national interests of Ukraine in cyberspace, main goals, directions and principles of state policy in cybersecurity , the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, the basic principles of coordination of their activities to ensure cybersecurity (Law Of Ukraine «On Basic Principles Of Cyber Security Of Ukraine»). Undoubtedly, this Law establishes general provisions and defines the main aspects of cybersecurity in Ukraine, but this Law is not a legal tool for practical application in the event of cyber attacks.

According to paragraph 5, part 1 of Article 1 of the Law of Ukraine «On Fundamentals of Cyber Security of Ukraine» cybercrime (computer crime) – a socially dangerous crime in cyberspace and / or with its use, liability for which is provided by the Law of Ukraine on Criminal Liability and / or which is recognized as a crime by international treaties of Ukraine. This law also specifies the objects of cybersecurity, cybersecurity and critical

infrastructure, which are subject to cybersecurity, and the legislator defines the subjects of cybersecurity protection and their powers (Law Of Ukraine «On Basic Principles Of Cyber Security»).

Cybercrime is cross-border in nature, so most states are interested in stopping actions against the leakage of personal data of their citizens on the Internet, and are interested in reducing the number of cyber attacks that interfere with public authorities, hospitals, banks and businesses. In fact, there is a high probability of going unpunished by seizing information that is a state secret, funds from well-known world companies through cyberattacks and interfering in the election process of another country.

Therefore, the effective fight against cybercrime requires greater, faster and more effective international cooperation, and therefore there is a need to unite countries to jointly fight cybercrime in the world (Tkachuk, 2020).

An important piece of legislation that plays a key role in the system of measures to combat cybercrime is the Convention on Cybercrime of November 23, 2001, which was ratified in Ukraine, provides for four groups of crimes involving the use of computer technology as a tool to commit them. The first group includes crimes against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, influence on data, influence on the functioning of the system, as well as illegal use of devices and computer programs). The second group includes crimes related to the use of computer tools (forgery, fraud). The third group includes crimes related to the content of the data. The fourth includes crimes related to copyright and related rights (Cyber Crime Convention, 2001).

In our opinion, the Directive on Network and Information Security, which sets out the general approach and rules of the European Union in the field of cybersecurity (Directive Of The European Parliament And The Council Of The European Council, 2016), needs to be implemented into national legislation. This document is aimed at intensifying cooperation on cybersecurity between the countries of the European Union. We believe that confidential data is the main target of cybercrime attacks.

The General Data Protection Regulation (GDPR) can also be considered a cybersecurity legal standard. After all, in the case of compliance with the requirements of the Regulations, the level of protection of personal information in the digital environment is significantly increased. Therefore, an important task for most countries in the coming years is to develop ways to implement the accepted norms in the field of cybersecurity in practice, which will help reduce cybercrime in the world.

In Ukraine, cybersecurity policy is entrusted to a number of government agencies, namely the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the

Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine. Relevant subdivisions operate in each of these bodies.

Despite the large number of criminal proceedings, the Cyberpolice Department does not announce the real results of such investigations. Indicating in the report the number of identified offenders in the amount of 800 people, there is no information about the number of actual sentences against these people and bringing them to justice. It is not clear from the report whether all these individuals have been declared suspects, whether charges have been filed and in what status they are (Nikulesko, 2019).

According to the Convention on Cybercrime, cybercrimes are conditionally divided into four types. The first type includes offenses against the confidentiality, integrity and availability of computer data and systems. This type of cybercrime includes all crimes against computer systems and data (for example, intentional access to a computer system or part thereof; intentional damage, destruction, deterioration, alteration or concealment of computer information; intentional commission, not having the right to manufacture, sell, purchase for use, distribute or otherwise make available devices, including computer programs).

The second type of cybercrime includes computer-related offenses. Such crimes are characterized by an intentional act that results in the loss of another person's property by any introduction, alteration, destruction or concealment of computer data or any interference with the operation of a computer system, with fraudulent or dishonest acquisition, without having to it is a right, an economic advantage for oneself or another person.

The third type of cybercrime covers offenses related to content (content), which is the commission of intentional illegal acts to produce, offer or provide access, distribution of child pornography, as well as possession of such files in their system.

The fourth type is intentional actions related to infringement of copyright and related rights, in accordance with the requirements of the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Agreement, as well as national legislation of Ukraine.

There are also other classifications of cybercrime, but the proposed convention is the most popular.

3.3. Criminal law mechanisms of fight against cybercrime in Ukraine

The main articles of the Criminal Code of Ukraine, which investigate cybercrime in Ukraine: Art. 176 «Infringement of copyright and related rights»; Art. 190 «Fraud»; Art. 361 «Unauthorized interference in the work of electronic computers (computers), automated systems, computer networks or telecommunication networks»; Art. 361-1 «Creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale»; Art. 361-2 «Unauthorized sale or dissemination of restricted information stored in computers, automated systems, computer networks or on such media»; Art. 362 «Theft, misappropriation, extortion of computer information or its acquisition by fraud or abuse of office»; Art. 363 «Violation of the rules of operation of automated electronic computer systems»; Art. 3631 «Interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks through the mass dissemination of telecommunication messages».

In Ukraine, the most complete statistics on cybercrime are reflected in the departmental statistical reporting of the National Police of Ukraine, in particular in the Report on the results of the National Police, where, in addition to crimes under Ch. XVI of the Criminal Code, designated and others committed with the use of electronic computers: "Infringement of copyright and related rights" (Article 176); "Theft" (Article 185); "Fraud" (parts 3 and 4 of Article 190). This category also includes crimes under Articles 200, 229, 231, h. 3, 4 and 5 of Art. 301 of the Criminal Code of Ukraine (Criminal Code of Ukraine).

In addition, certain indicators of cybercrime under other articles of the Criminal Code are reflected in other statistical reports, in particular the crimes under Art. 3761 "Illegal interference in the work of the automated document management system of the court" – in the Unified Report on Criminal Offenses, which is prepared by the Office of the Prosecutor General of Ukraine.

Section II "Participation of services and units of the National Police in the disclosure of criminal offenses (by type), the pre-trial investigation of which is completed" reflects the results of disclosure (investigation) of criminal offenses under the Criminal Code: "Forgery of documents, seals, stamps and forms, as well as the sale or use of forged documents, seals, stamps"; Crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors, etc. Thus, not all traditional crimes committed with the help of computer technology and the Internet are reported as cybercrime.

Some Ukrainian scientists consider cybercrime to be crimes under Articles XVI of the Criminal Code and crimes, the indicators of which are reflected in the report of the National Police of Ukraine.

However, some scientists, in particular Professor AV Savchenko, believe that in addition to the offenses listed in the report, the category of cybercrime may include others under the Criminal Code of Ukraine, provided that the tool for their commission were information network technologies and (or) their consequences will be reflected in cyberspace (Savchenko, 2001).

Cybercrime may include the following: acts aimed at forcible change or overthrow of the constitutional order or the seizure of state power (Article 109); encroachment on the territorial integrity and inviolability of Ukraine (Article 110); treason (Article 111); sabotage (art. 113); espionage (art. 114). The acts provided by such articles of the Criminal code can be carried here also: 132; 145; Part 1 of Art. 158; 159; 161; 163; 168; 182; 232; 259; 263; 295; 300; 303; 307; 312; 313; 328; 330; 345; 3451; Part 1 of Art. 346; Part 1 of Art. 350; Part 1 of Art. 376; 381; 387; Part 1 of Art. 398; 422; 436 (Criminal Code of Ukraine).

The object of cybercrime is public relations, which are harmed by the impact on information circulating in cybernetic systems. The subjects of computer crimes are multifaceted and are determined depending on the norm of the article that falls under the act, but unites them one – they are information that, in various forms, circulates in computer networks, systems and computer networks, telecommunication networks (Richka, 2019).

In our opinion, certain provisions of the legislation should be unified in order to avoid misunderstandings in the definition of acts that fall under the characteristics of crimes in the use of computers, systems and computer networks and telecommunications networks and cybercrime as a whole. Based on the existence in the Convention on Cybercrime and the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» of the concept of «cybercrime (computer crime)», it is necessary to change the title of Chapter XVI of the Criminal Code of Ukraine «Crimes in the use of computers, systems and computer networks and telecommunication networks «on» Cybercrime».

It is also worth pointing out certain problems with the qualification of cybercrime. According to experts, the main criterion for distinguishing the crimes provided for in Articles 361363-1 of the Criminal Code from others related to the use of computer equipment as a tool or means of committing a crime is the object of encroachment. Thus, the peculiarity of the criminal qualification of crimes against property committed with the use of computer equipment is the need to address the issue of the appropriateness of additional qualification of the perpetrator's actions under articles providing for liability for crimes in the use of computer equipment.

In this case, it should be guided by the fact that the use of computer equipment in committing crimes against property forms an independent crime only when certain damage is caused to the object – the relationship of ownership of computer information, when certain information was illegally destroyed, blocked, modified. And in those cases when certain information systems are used for their intended purpose, additional qualifications are not needed (Gutsalyuk, 2019).

There is also now a problem of criminal qualification of actions that computer users perform in the field of cryptocurrency circulation and the use of artificial intelligence.

Thus, in March 2018, researchers from RWTH Aachen University (Germany) found that the Bitcoin blockchain contains about 1,600 files, where there are scenes of child abuse, with at least 8 files with pornographic content. The blockchain contains external links to 274 video files on child abuse and about 142 links to darkweb. According to scientists, the finding may outlaw the blockchain, but today there are no court rulings in this regard, apparently due to the complexity of criminal law. Anyone who participates in the Mining procedure or owns bitcoins can be involved in the appearance of pornographic content on the network (In Bitcoin Blocks Found Trace Of Child Pornography, 2018).

In practice, law enforcement and judicial officials have many problems qualifying cybercrime. This is especially true in cases of committing this type of crime, encroaching on several objects protected by criminal law.

Most often, errors are found in the qualification of one act, which, at first glance, contains signs of several types of crimes. Thus, the main problem here is to determine the presence or absence in the perpetrator of an ideal set of crimes.

During the commission of a cybercrime, damage may be inflicted on: 1) public relations arising in the course of ensuring (with the help of information and telecommunication systems) the vital activity of a person, society, or the state; 2) traditional public relations, which are provided by information and telecommunication systems; 3) traditional public relations, protected by law, for the harm of which information and telecommunication systems are used, which are not harmed.

The first group of relations is protected by Section XVI of the Special Part of the Criminal Code. These relations are part of the second and third groups of relations, but in the second group they are harmed together with the traditional relations of criminal law protection, and in the third - no.

The ideal set of crimes is considered to be two or more crimes committed in one act. According to the specified groups of relations which are harmed at commission of such act in case of commission of a cybercrime,

it is possible to allocate three groups of these crimes which will have the features of qualification according to the operating Criminal code: 1) crimes in the sphere of use of computers, their systems, computer networks , telecommunication networks; 2) crimes qualified under the relevant article of the Criminal Code based on the object of encroachment with additional reference to the articles of Chapter XVI of the Criminal Code; 3) crimes qualified under articles of the Criminal code according to object of encroachment without the additional reference to articles of section XVI of the Criminal code of Ukraine.

That is, actions with the first and third groups are single crimes, and with the other – an ideal set of crimes. But in the practice of applying the provisions of the Criminal Code in combating cybercrime, acts belonging to different of these groups are often confused. Most often, crimes of the second group are classified under only one article, and vice versa, crimes of the first or third group are classified under several articles, although they do not require additional qualification.

Thus, the article is applied at qualification of the second group of crimes or from section XVI of the Criminal code, or another - according to direct object of encroachment. It is obvious that in both cases the part of the crime of qualification is not covered, which violates the principles of completeness and accuracy of qualification, and in the case of qualification of one act containing one crime under two articles, the principle of prohibition of double incrimination is violated.

As the generalization of judicial practice shows, a significant part of cybercrime occurs in cases where the encroachment on the use of information and telecommunications systems is carried out for selfish motives to steal or seize someone else's property with material damage and is a way to commit property crimes such as fraud (Article 190 of the Criminal Code of Ukraine) or misappropriation or seizure of property through abuse of office (Article 191 of the Criminal Code of Ukraine). In most cases, courts classify the following actions as a set of crimes: under Article XVI of the Criminal Code and the article that provides for liability for a specific crime against property, the method of which was the use of information and telecommunications systems.

However, in some cases, the courts classify these actions only under the articles of Chapter XVI of the Special Part of the Criminal Code of Ukraine.

The authors of the generalization believe that in the latter case, since E. repeatedly fraudulently seized funds through illegal transactions using computer technology, and interference in the work of computer technology is a way of committing a crime against property, such actions need additional qualifications Art. 190 of the Criminal Code of Ukraine (fraud). We believe that there really is a set of crimes, but it is already taken into account in the

Criminal Code in Part 3 of Article. 190, therefore, qualification under this norm is required without additional references to the norms of the Criminal Code (Hrytsiv, 2007).

One of the common problems of criminal law qualification is the question of the qualification of the ideal set of crimes, namely the absorption of one crime by another, which was part of it. This problem still requires a solution by scientists. In particular, T. Sozansky formulates a rule in relation to crimes that have additional objects of encroachment: a set of crimes. " But it is further pointed out that it is quite difficult to determine when an object is additional and when it becomes the main one, especially when assessing cybercrime. He proposes, as an option to address this issue, to determine the public danger of encroachment on the relations that are protected by these objects. If the social danger of the relations protected by the additional object is greater than the main object, then the act forms an ideal set (Sozansky, 2009).

In our opinion, Section XVI of the Criminal Code of Ukraine should be supplemented with qualifiers for committing computer crimes by organized groups and criminal organizations, increasing criminal liability for use of official position, not only to Article 362 of the Criminal Code, but also to other provisions of the section. It is advisable to qualify according to the set of norms of the Criminal Code under Article XVI of the Criminal Code and Article 255 of the Criminal Code of Ukraine and against the background of increased public danger.

We also share D. Richka's point of view that in connection with the emergence of new types of computer crimes, the provisions of the Criminal Code of Ukraine should be supplemented with the following crimes: in the field of financial crimes: skimming, cash trapping, carding; in the field of e-commerce and economic activity - phishing; in the field of intellectual property: piracy, cardsharing; crimes in the field of information security (Richka, 2019).

Also, according to M. Karchevsky, the lack of legal certainty regarding the use of cryptocurrency has a negative impact on the prospects for the development of the IT sector of the economy. This sector is developing most dynamically and is promising given the significant investment in Ukraine's economy. The legal ban on the use of cryptocurrency in Ukraine will not solve these problems, but only create new ones, as Cryptocurrency will be increasingly used by criminals and corrupt people precisely because of its illegal status, while the opportunities for law enforcement, for the same reason, will be significantly limited (Karchevsky, 2017).

At the same time, it should be emphasized that the main issue of criminal law regulation in the field of information resource formation is a clear and consistent definition of the limits of opportunities for effective influence on

public relations by means of criminal law. The multidimensionality and scale of the damage from the uncontrolled information space is beyond doubt. However, it is hardly expedient to solve these problems by supplementing the Criminal Code with new norms.

Proposals to impose penalties for various forms of manipulation of public consciousness are controversial due to the projected inefficiency and declarativeness, their inconsistency with the principles of criminal-political adequacy, as well as the proportionality of positive and negative consequences of criminalization. In addition, the spread of global information technology in general makes methods of restricting or banning content less effective. The solution of the problem is beyond the scope of criminal law regulation and, in our opinion, involves, first of all, systematic work in the field of education and the formation of competitive information products (Karchevsky, 2017).

The growing trend of cybercrime and the trend of «lagging behind» social and legal control over it create an extremely great civilizational threat, which can be overcome only through an organic combination of criminal law and forensic strategies to combat this type of crime. Moreover, as E. Skulish rightly points out, an important component of such a strategy should be more transparent and operational international cooperation in this area, as it is already obvious that it is impossible to control the transnational component of cybercrime and cyberterrorism at the state level. In fact, this set of problems must be addressed immediately by the international community in the XXI century (Skulish, 2014).

In the modern information society, where cyber threats are widespread and will continue to spread, it is important to constantly and systematically, in a timely manner to take effective measures to combat cybercrime, as well as to improve its methods and forms of prevention. This applies to almost all spheres of public and state life, business and socio-humanitarian environment. Given Ukraine's course to enter the global information space, V. Shemchuk expressed the belief that a national model for cybersecurity of enterprises, institutions and organizations, including non-governmental ones, needs to be built; coordination of efforts and interaction of law enforcement agencies, special services, the judiciary, as well as their proper staffing and logistics, exchange of information on the prevention and fight against cybercrime (Shemchuk, 2018).

It should be noted that in order to fulfill its obligations to the European Union, Ukraine is currently carrying out an unsystematic rule-making process by amending and supplementing existing domestic legislation instead of creating and developing basic regulations in the field of information law. In this light, the process of adaptation of Ukrainian legislation creates even more legal conflicts and gaps in the already imperfect domestic legislative array.

To sum up, cybercrime has become a challenge of the 21st century, which can be combated only through joint efforts and not only at the interstate level, but also within the state within the framework of cooperation between the public and private sectors. Given the cross-border nature of cybercrime, it requires the establishment of law enforcement cooperation in the investigation of cybercrime at the operational level; creating and ensuring the functioning of the mechanism for resolving jurisdictional issues in cyberspace.

Along with the listed areas, the criminal law support of the fight against cybercrime needs to be further improved, the implementation of international standards into national legal norms. In addition, the qualification of cybercrime has its own characteristics that must be taken into account. These and other problems in the fight against cybercrime are far from exhausted, they can be considered at international scientific conferences, as well as be the subject of further research.

3.4. Detection and forensic support in the fight against cybercrime in Ukraine

According to Part 3 of Article 7 of the Law of Ukraine «On operational and investigative activities» detection as a type of activity precedes the investigation (On Operational And Exploratory Activity: Law Of Ukraine, 1992).

Today in Ukraine it is possible to identify such subjects of operational and investigative activities that directly or indirectly detect cybercrimes, such as the National Police of Ukraine and the Security Service of Ukraine.

According to § 3 of the Cyber Security Strategy of Ukraine, the National Police of Ukraine belongs to the National Cyber Security System as a body that protects human and civil rights and freedoms, interests of society and the state from criminal encroachments in cyberspace and implements measures to prevent, detect, stop and disclose such crimes. As subjects of cybercrime detection, structural units of the National Police can be divided into two groups:

1) operational units of the Cyberpolice Department are directly obliged to carry out operational and investigative activities by their own methods in order to combat conventional crimes (responsibility for which is actually provided by Articles 163, 176, 185, 190, 200, 301, 361-363-1 of the Criminal Code of Ukraine) (Criminal Code Of Ukraine).

2) other operational units of the National Police (Department of Criminal Investigation, or Department of Economic Protection, or Department of Counteraction to Drug Crime, etc.) that counteract

other, alternative to the Convention, crimes committed in cyberspace and investigated by investigators of the National Police of Ukraine.

The Department of Cyberpolice in relation to such crimes can only assist in the manner prescribed by applicable law, other units of the National Police of Ukraine in the prevention, detection and cessation of criminal offenses - ensures timely receipt of information about crimes committed in cyberspace or related criminal intent

Units of counterintelligence protection of interests of the state in the field of information security, protection of national statehood of the Security Service of Ukraine. The tasks of the Security Service also include the prevention, detection, cessation and detection of crimes against peace and security of mankind, terrorism, corruption and organized crime in the field of government and economy and other illegal actions that directly threaten the vital interests of Ukraine.

From the standpoint of investigative practice, the procedural procedure for initiating criminal proceedings continues from the moment when the subject of investigation became aware of the source of circumstances that may indicate a criminal offense, until he enters information into the Unified Register of Pre-trial Investigations.

The internal organization of investigators at the beginning of criminal proceedings will depend on two factors: legal and non-legal (organizational). The legal factors that determine the forms of initiation of criminal proceedings are related to the nature of the source of circumstances that may indicate the commission of a certain type of criminal offense. Peculiarities of using the functionality of operative-investigative activity for the purpose of detecting a criminal offense are organizational factors that determine the peculiarities of the form of initiation of criminal proceedings for a particular type of crime (Samoylenko, 2020).

Scholars single out the following main organizational forms of initiating criminal proceedings: 1) criminal proceedings were instituted at the request of the victim / notification of a person about a criminal offense (non-alternative form); 2) criminal proceedings were instituted on the basis of materials of operational units obtained as a result of verification of operational information (alternative form) - recognized the complexity of the implementation of verification materials on minor and moderate crimes, which explains the formality of non-alternative form of proceedings; 3) criminal proceedings have been instituted within the framework of the implementation of the materials of the operational search case (non-initiative form) – its prevalence in relation to crimes committed in cyberspace for political reasons, crimes that violate the established order of certain things; 4) criminal proceedings were instituted as a result of detecting a crime committed in cyberspace during the investigation

of another criminal proceeding (initiative form) – its atypicality was recognized, the investigator detects such crimes, usually by accident (Samoylenko, 2020).

In order for information about the commission or preparation of a cybercrime to have the prospect of a pre-trial investigation, it must be confirmed by reliable sources for the investigator. An important component of providing operational units with evidence in criminal proceedings on the fact of cybercrime is the documentation of relevant facts, which is carried out during both operational and investigative activities, and the implementation of operational units instructions of the investigator, prosecutor to conduct covert investigative (investigative) actions. The main operational search methods for detecting criminal offenses in the field of drug trafficking are as follows: controlled delivery; controlled and operational procurement; establishing confidential cooperation; intelligence survey; operational monitoring.

The result of the documentation is the creation of documents that, after appropriate assessment and verification by the investigator, the prosecutor can be used as evidence in criminal proceedings. Such results can be used both to provide evidence in specific criminal proceedings and for other purposes established by the Criminal Procedure Code and the Law of Ukraine «On operational and investigative activities» (Sakovsky and Klimchuk, 2019).

It should also be noted that the detection of such criminal offenses involves obtaining the most complete and reliable information about the signs of preparation or commission of criminal offenses of this kind by identifying the appropriate media. The main means of gathering evidence in the field of criminal justice are investigative (search) actions. The Criminal Procedure Code of Ukraine explicitly states in Art. 93, which states that the prosecution collects evidence by conducting investigative (investigative) and covert investigative (investigative) actions, and the defense, the victim, a representative of the legal entity in respect of which the proceedings may initiate them by submitting to the investigator, prosecutor relevant petitions (Criminal Procedural Code Of Ukraine, 2012).

In the course of such an investigative (search) action as a search, there is a need for qualified detection, recording and removal of such information or its media, taking measures to prevent external (external) influence on electronic traces of crime (eg, power outages, remote access to files and system management, etc.), readiness of investigative bodies to promptly conduct investigative (search) actions in other places where digital information may be stored.

In our opinion, which is based on the results of the relevant survey of practitioners, specific conditions for the search and seizure of electronic

evidence should be introduced. First of all, we see the need to determine the procedurally significant possibility of copying data. Articles 16-18 of the Cybercrime Convention need to be introduced into domestic law, namely the immediate recording and subsequent storage of data by operators, telecommunications providers, hosting providers, resource owners (website, web pages, etc.) to ensure their integrity.

The implementation of the provisions of Article 19 (Search and Seizure of Stored Computer Data) of the Convention on Cybercrime will increase the effectiveness of cybercrime investigations by strengthening the ability to copy, retrieve and block / arrest electronic data. Given the observance of international standards for the protection of owners and users of such information, it is necessary to ensure proper judicial review at the pre-trial stage. Therefore, it is expedient to carry out the relevant procedural actions on the basis of the decision of the investigating judge, the court, and the factual data obtained in such ways to be considered admissible evidence in criminal proceedings.

Of course, these are not all the problems that exist in the practice of detecting and investigating cybercrime in Ukraine. Unfortunately, the requirements for the scope of this type of work, such as a scientific article, do not allow for a detailed analysis of this issue. At the same time, it will encourage other scientists to find ways to optimize the investigation of cybercrime.

Conclusions

The scientific article outlines the features inherent in the criminal law qualification of cybercrime, identifies criminal law and forensic mechanisms to combat cybercrime, developed proposals to improve existing legislation.

At the conceptual level, the search for ways to increase the effectiveness of the fight against cybercrime is to resolve conflicts in the field of legal regulation of the information space and create common rules for its use in both private and corporate interests.

With the introduction of the institute of criminal offenses into the national criminal legislation, the terms «cybercrime» and «computer crime» have lost their relevance, which indicates the expediency of making appropriate terminological changes to the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» and other regulations. part of the use of the term «cyber offense», which should be understood as a socially dangerous crime in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or recognized as a criminal offense by international treaties of Ukraine.

Based on the existence in the Convention on Cybercrime and the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» of the concept of «cybercrime (computer crime)», it is necessary to change the title of Chapter XVI of the Criminal Code of Ukraine «Crimes in the use of computers», systems and computer networks and telecommunication networks «on» Cybercrime».

In connection with the emergence of new types of computer crimes, the provisions of the Criminal Code of Ukraine should be supplemented by the following crimes: in the field of financial crimes: skimming, cash trapping, carding; in the field of e-commerce and economic activity – phishing; in the field of intellectual property: piracy, cardsharing; crimes in the field of information security.

Section XVI of the Criminal Code of Ukraine is also to be supplemented by qualifying bodies for committing computer crimes by organized groups and criminal organizations, increasing criminal liability in the use of official position, not only to Article 362 of the Criminal Code of Ukraine, but also to other provisions of the section. Due to the increased public danger, it is advisable to qualify according to a set of rules – under Article XVI of the Criminal Code of Ukraine and Article 255 of the Criminal Code of Ukraine «Creation, management of a criminal community or criminal organization, as well as participation in it».

Thus, the formation of an effective system for combating cybercrime in Ukraine requires systematic measures at both the conceptual and organizational and legislative levels: at the conceptual level – to identify the main threats to cybersecurity and formulate measures to prevent and prevent them; at the organizational level - to determine a single body for operational management of all entities whose task is to ensure cybersecurity (cyber units of law enforcement agencies) in peacetime, to create a system of technological means of the national cybersecurity system, to establish closer international cooperation; at the legislative level – to implement in national legislation the Directive on Network and Information Security, which sets out the general approach and rules of the European Union in the field of cybersecurity, and in the field of criminal law – to streamline legislation on the use of common terminology. In the information space in order to comply with its international standards.

In order to increase the effectiveness of the investigation of cybercrime by law enforcement agencies of Ukraine: argued the feasibility of active use of operational and investigative sources of information about cybercrime; proved the need to detail the legislation that would reflect the provisions of the Convention on Cybercrime, on obtaining electronic evidence, restricting (blocking) a certain information resource (information service), specific conditions of search and seizure of digital (electronic) evidence.

Bibliographic References

CARPENTER, Oksana. International legal problems of definition and classification of «cybercrimes». Available online. In: http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf. Consultation date: 02/04/2022.

CRIMINAL CODE OF UKRAINE. Available online. In: http://zakon3.rada.gov.ua/ laws / show / 2341-14 / page. Consultation date: 04/04/2022.

CRIMINAL PROCEDURAL CODE OF UKRAINE. 2012. Law of Ukraine of April 13, 2012 № 4651-V1. Available online. In: http://zakon.rada.gov.ua/go/4651-17. Consultation date: 04/02/2022.

CYBER CRIME CONVENTION. 2001. Available online. In: https://zakon.rada.gov.ua/laws/show/994_575#Text. Consultation date: 01/02/2022.

CYBERCRIME, LEGAL REGULATION. Available online In: https://ua.interfax.com.ua/news/press-release/756785.html Consultation date: 04/04/2022.

EU INTERNATIONAL CYBERSPACE POLICY. Available online. In: http://www.eeas.europa.eu/ policies / eu-cyber-security / index_en.htm. Consultation date: 04/02/2022.

GUTSALYUK, Mykhailo. 2019. Scientific and practical commentary on the Law of Ukraine «On the basic principles of cyber security of Ukraine». National Academy of the Prosecutor's Office of Ukraine. Kyiv, Ukraine.

HOME AFFAIRS COMMITTEE E-CRIME FIFTH REPORT OF SESSION 2013–14. Available online. In: https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/869/869.pdf Consultation date: 04/02/2022.

HRYTSIV, Mykhailo. 2007. Generalization of the Supreme Court of Ukraine. In: http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02. Consultation date: 04/04/2022.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013 Available online. In: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001. Consultation date: 04/02/2022.

KARCHEVSKY, Mykola. 2017. "The main problems of criminal law regulation in the field of informatization" In: Bulletin of LDUVS named after E.O. Didorenko. Vol. 79, No. 3, pp. 67-78.

KOZYCH, Igor. 2020 Criminal law policy: functions and functioning. Monograph. Ivano-Frankivsk, Ukraine.

MCGUIRE, Mike; DOWLING, Samantha. 2013. Cybercrime: A review of the evidence Summary of key findings and implications. Available online. In: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Consultation date: 04/02/2022.

NIKULESKO, Dmitry. 2019. Cybersecurity: vulnerabilities. Available online. In: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html Consultation date: 04/02/2022.

ON MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ON THE TERRITORY OF THE UNION. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF THE EUROPEAN UNION. 2016. 2016/1148 of 6 July 2016. Available online. In: https://zakon.rada.gov.ua/laws/show/984_013-16#Text Consultation date: 04/02/2022.

ON OPERATIONAL AND EXPLORATORY ACTIVITY. 1992. Law of Ukraine of February 18, 1992 №2135-12. Available online. In: http://zakon2.rada.gov.ua/laws/show/2135-12. Consultation date: 04/02/2022.

ON THE BASIC PRINCIPLES OF CYBER SECURITY IN UKRAINE. 2017. Law of Ukraine of October 5, 2017 № 2163-VIII. Available online. In: https://zakon.rada.gov.ua/laws/show/2163-19. Consultation date: 04/04/2021.

PRESIDENT'S DECREE «ON THE DECISION OF THE COUNCIL OF NATIONAL SECURITY AND DEFENSE OF UKRAINE OF JANUARY 27. 2016. «ON THE CYBER SECURITY STRATEGY OF UKRAINE». Available online. In: https://www.president.gov.ua/documents/962016-19836. Consultation date: 04/04/2021.

RICHKA, Denis. 2019. Features of criminal-legal qualification of crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks. University of the State Fiscal Service of Ukraine, Irpin. Dnipro, Ukraine.

SAKOVSKY, Andriy; KLYMCHUK, Mykhailo. 2019. "Features of documentation of criminal offenses related to illicit trafficking in narcotic drugs, psychotropic substances, precursors and their analogues" In: Law Journal. National Academy of Internal Affairs. No. 2, pp. 49 59.

SAMOYLENKO, Olena. 2020. Detection and investigation of cybercrime: a textbook. Odesa, Ukraine.

SAVCHENKO, Andriy. 2001. "Combating computer crimes: criminal law and tactical forensic aspects" In: Actual problems of legal sciences in researches of scientists. No. 11, pp. 9-14.

SHEMCHUK, Victor. 2018. "Cybercrime as an obstacle to the development of the information society in Ukraine" In: Scientific notes of TNU named after VI Vernadsky. Series: legal sciences. Vol. 29, No. 6, pp. 119-124.

SKULISH, Eugen. 2014. "International legal cooperation in the field of combating cybercrime" In: «Information and Law». Vol. 10, No. 1, pp. 93-100.

SOZANSKY, Taras. 2009. Qualification of a set of crimes; Lviv State University of Internal Affairs. Lviv, Ukraine.

TENTH UNITED NATIONS CONGRESS ON THE PREVENTION OF CRIME AND THE TREATMENT OF OFFENSES. 2000. Vienna, 10-17 April. Available online. In: https://undocs.org/pdf?symbol=ru/A/CONF.187/4/REV.3. Consultation date: 04/04/2021.

TKACHUK, Maryana. 2020. The concept of cybercrime in Ukrainian and international law. Available online. In: http://jurfem.com.ua/ponyattya-kiberzlochynnosti-v-ukrainskomu-ta-mizhnarodnomu-zakonodavstvi-tkachuk-mariana/. Consultation date: 04/01/2022.

TRACES OF CHILD PORNOGRAPHY WERE FOUND IN BITCOIN BLOCKS. 2018. Available online. In: https://www.volynnews.com/news/all/u-blokakh-Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-/. Consultation date: 04/01/2022.

UN ECONOMIC AND SOCIAL COUNCIL. 2001. Commission on Crime Prevention and Criminal Justice. Vienna 8-17 May. Available online. In: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_10/E-CN15-2001-01/E-CN15-2001-1_R.pdf. Consultation date: 04/02/2022.

UNIFIED REPORT ON CRIMINAL OFFENSES IN THE COUNTRY: the official website of the Prosecutor General's Office of Ukraine. Available online. In: https://www.gp.gov.ua/ua/stat_n_st?dir_id=113897&libid=100820&c=edit&_c=fo Consultation date: 04/02/2022.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.40 Nº 73

Esta revista fue editada en formato digital y publicada en julio de 2022, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org