UDC 343.9.024:338.28 doi: https://doi.org/10.33270/01191101.58

Hrebeniuk M. – Ph.D in Law, Associate Professor, Head of the Interagency Scientific and Research Centre on Problems of Combating Organized Crime under National Security and Defense Council of Ukraine, Kyiv, Ukraine;
ORCID: https://orcid.org/0000-0003-1249-5576;

Cherniak A. – Doctor of Law, Chief Researcher Fellow of the Interagency Scientific and Research Centre on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine, Kyiv, Ukraine;
ORCID: https://orcid.org/0000-0002-4958-783X

Countering the Use of Leading Sectors of Digital Economy by Organized Crime: European Experience

The digital economy on a global scale is developing at a fast pace and acts as an accelerator of innovation, competitiveness and economic growth in the world. Most of the advanced countries of the world, such as the USA, Canada, Japan, and Germany are developing the digital economy and introducing digital technologies in their societies as a strategic goal, which in the future should be the driving force of innovation development, including for the Ukrainian economy. The ***purpose*** *of the article is to highlight the European experience of preventing and countering organized crime in the digital economy, carrying out an analysis of the novels of modern legislation. The theoretical basis and scientific issues of the chosen scientific direction were considered in the fundamental works of such scholars as: V. M. Butuzov, M. O. Budakov, S. V. Demediuk, V. V. Markov, A. I. Marushchak. Law enforcement agencies should have the tools, methods and experience to combat the criminal misuse of encryption and anonymity methods. To prevent criminals from using encryption and anonymization methods, law enforcement agencies should retrain personnel, and not only employees of units engaged in combating cybercrime, and also have at their disposal the necessary software and hardware systems. In addition, law enforcement officers should be provided with the necessary software tools that allow the use of cyber tools to investigate not only particularly complex, but also any crimes in digital format.* ***Conclusions.*** *Currently, the main task for which the digital economy is aimed is the introduction of digital technologies in industrial production, education, medicine and other fields. It's common knowledge that the sectors of the economy that use digital technology are developing faster and better. Spheres of human activity, including education, medicine, transport, agriculture, are being modernized thanks to digital technologies, becoming much more efficient and creating new value and quality. Indeed, the continuous development of digital technologies is also one of the reasons for the increase in the scale of the shadow economy, since along with the development of modern technologies, new opportunities for the growth of «digital crime» are emerging. Assessing the impact of the «digital economy» on the national and world economy, as well as inevitably on the entire social sphere, is very important, given the growing problems of the spread of transnational crime in the virtual space, which is also being modernized on a permanent basis. The basis of the development of the digital economy is the blockchain technology, which finds its application in various fields. Describing the state of organized crime in the economic sphere, it is advisable to allocate it in a separate category for the study of crime in the sphere of the «digital economy». Evaluation of the impact of the digital economy on the national and world economy allows us to state that the continuous modernization of crime remains relevant, which is constantly being improved as part of the active continuous electronicization and digitalization of society. Another factor that should be considered when countering crimes in the «digital economy» is the enormous victimization rate.*

Keywords: counteraction; organized crime; digital economy; European experience; innovations; law enforcement agencies; victimization.

Introduction

An important component of the formation of an information society is the use of the capabilities of modern ICT to create information, new modern knowledge, goods and electronic services, effective information exchange, while promoting the stable development of the country. ICT application in the conditions of intensive development of market relations remains one of the important elements of good governance. Over the past decade considerable attention has been paid in empirical economics to testing for the existence of relationships in levels between variables. In the main, this analysis has been based on the use of integration techniques. Financial stability within the framework of the global financial crisis has become a common topic for researchers and practitioners (Stoica & Ihnatov, 2016). The development of the digital economy in Ukraine consists in creating market incentives, shaping the needs for using digital technologies, products and services among Ukrainian industrial sectors, spheres of life, business and society for their efficiency, competitiveness and national development, growth of high-tech production and well-being of the population. That is, digital transformation is a process that must be one of the priorities for modern development.

Selected for the study of scientific issues, from different points of view studied by many scholars. Special attention is paid to the chosen issues in the legislation of the leading European countries. The study of the state of scientific development of the problems of cooperation and interaction of the competent authorities of different countries in counteracting the use of organized crime by leading sectors of the digital economy was highlighted by domestic scientists.

Selected for the study of scientific issues from different points of view has been studied by many scientists. Certain aspects of this scientific direction were considered in the fundamental works of such scientists as: V. M. Butuzov, M. O. Budakov, S. V. Demediuk, V. V. Markov, A. I. Marushchak, Yu. Ye. Maksymenko, O. V. Orlov, S. M. Rohozin, V. S. Tsymbaliuk etc.

The purpose

The purpose of the article is to highlight the European experience of preventing and countering organized crime in the digital economy, carrying out an analysis of the novels of modern legislation.

Objectives of the study

A generalization of the existing research results on selected topics and its coverage, taking into account the best practices of the latest European legislation on combating the use of organized crime by the leading sectors of the digital economy, which simultaneously indicates the relevance and timeliness of the scientific research carried out by the authors of the scientific paper.

Presentation of the main material

Commonly used both in the world and in the European Union (EU) countries, *the definition of «digital economy»* is interpreted as electronic commerce, carried out with the help of modern information and communication technologies. In particular, the *Bank of England* looks at the management models of the monetary system from the position of the dynamic blockchain development. *In Estonia,* blockchain is also being actively introduced into the banking system, and besides – into the health care system and state registration of business activities. *Australia Post* intends to use the blockchain to store the digital identification data of its customers. *In Switzerland and the United Kingdom,* a favorable environment has been created for the development of the latest technologies «FinTech» using «regulatory sandboxes» (modes of limited use of products in the absence of appropriate financial legislation).

In 2018, a revolutionary idea of creating a common digital market was documented in the European Union: 22 countries signed a joint declaration on the creation of a European blockchain partnership ("YeS pratsiuie"). This European project involves the exchange of information and technology between states and the private sector. This declaration is based on three main principles: unhindered access to digital products and services; creating an adequate environment for the dynamic development of network and digital technologies; taking advantage of the digital market as an important potential for accelerating economic growth.

Information and telecommunication networks can also be used to commit economic crimes related to the acquisition and sale of certain items, including counterfeit money, securities, bank cards, as well as data from existing bank cards. However, in this case, the use of the Internet or other information and telecommunication networks is one of the possible methods of committing relevant crimes. For example, the data of valid bank payment cards allows you to make purchases in online stores without using a special PIN code. On the Internet, for sale are actively offered bilateral images of bank cards, as well as their PIN codes, in the presence of which you can make a fake counterpart of such cards and use it to pay for goods in regular stores ("European Cybercrime").

Also through the Internet resources skimmers are sold and bought (devices installed on ATMs and allow you to read the data of a bank card that is used). Without a causal connection with a specific crime, many of these actions (for example, the provision of data from a valid bank card or the sale of a skimmer) are not criminalized, which is a gap in the law. Without a causal relationship with a specific crime, many of these actions (for example, the provision of data from a valid bank card or the sale of a skimmer) are not criminalized, which is a gap in the law. Organized cybercrime can be associated not only with information security problems, but also with threats to state security, the military-industrial and industrial complexes, and life-support infrastructure. With the active use of Internet services, electronic gadgets and modern means of payment, no one can feel safe. For example, the receipt of messages containing various kinds of fraudulent methods of defrauding information has become an integral part of everyday life today, while the overall assessment of the public danger of such acts rarely goes beyond the limits of petty hooliganism. That is, the practical achievements and achievements of the digital economy are actively used by transnational organized criminal groups in order to obtain superprofits by committing economic crimes in the

territory of one or several states using cyberspace and its capabilities.

As stated in the Europol report ***«Internet Organised Crime Threat Assessment» (IOCTA) (2018)*** (Liashenko, 2018), ensuring the rule of law in cyberspace requires intensifying work on the identification and localization of individual criminals and criminal groups that are integral elements of the modern European criminal subculture. The *IOCTA Strategic Report* provides key recommendations to law enforcement agencies, politicians and regulators so that they can effectively and consistently respond to and resist cybercrime. It is emphasized that the important components for the successful struggle of law enforcement agencies against cybercrime are such components as the allocation of sufficient resources for the study of malicious software and new business models of cybercrime, as well as conducting stress tests and security audits of state bodies and the public. Law enforcement agencies should have the tools, methods and experience to combat the criminal misuse of encryption and anonymity methods. To prevent criminals from using encryption and anonymization methods, law enforcement agencies should retrain personnel, and not only employees of units engaged in combating cybercrime, and also have at their disposal the necessary software and hardware systems. In addition, law enforcement officers should be provided with the necessary software tools that allow the use of cyber tools to investigate not only particularly complex, but also any crimes in digital format.

An important place is occupied by the prevention of organized crime in the field of advanced technologies. Currently, preventive cybercrime campaigns are aimed mainly at citizens and businesses, that is, potential victims of cybercrime. In addition, it is also necessary to intensify preventive work with potential cybercriminals, primarily teenagers and young people, who possess the necessary software skills, as well as IT workers. The focus of preventive work should be on explaining the consequences of illegal activities for the criminals themselves. It should be noted that national preventive campaigns should be coordinated with international and public organizations. As part of preventive activities, special attention should be paid to mobile gadgets and modern electronic devices as the sources of greatest danger to their owners and the penetration of criminals into private and corporate networks. Law enforcement agencies, together with non-profit organizations and the private sector, should be actively involved in awareness-raising activities among the public and the public (Kiberbezpeka, 2016).

One of the main tasks of the EU law enforcement agencies is to fight against providers of criminal services and specialized tools that are the basis of software, hardware and personnel structures of European cybercrime. These types of specialized tools include: malicious software, including password extortionists, spyware, and banking trojans, as well as, respectively, their developers, suppliers and customers, providers, organizers and performers of DDoS attacks as services; manufacturers of botnets, especially their modifications, used to distribute other malicious programs; carrying out DDoS attacks, as well as criminal manipulations by distorting and "noisy" information space.

Scientific novelty

The vast majority of criminal instruments and services can be used in a wide variety of areas of criminal activity. Accordingly, exposing and terminating the activities of criminal networks involved in the manufacture of software tools and provide services for their use in the interests of other criminal groups will allow countering cybercrime. It is no coincidence that while committing crimes in the digital economy, the key factor is the enrichment motive. Also in the conditions of crisis, there are frequent cases when dismissed employees of IT companies illegally encroach on information resources of an enterprise and transfer commercial secrets to competitors not so much from mercenary motives as for revenge, while material gain is of secondary importance. In the digital economy, criminal groups primarily resort to such forms of criminal activity: the use of phishing sites; falsification and forgery of electronic documents; malware distribution. Thanks to this illegal activity, one can gain access to the management of bank accounts of legal entities with the aim of gradually stealing money. Also in this category of crimes can be attributed to the theft of authentication data (digital signature), which allows you to get unhindered access to the accounts of electronic payment system agents, transfer financial resources from them to personal accounts of subscriber phone numbers, and then transfer them to cash.

Analysis and study of the scientific and analytical work of European criminological researchers makes it possible to state the dominance of the position according to which in modern conditions the sign of unity of organized groups is lost during crimes in the digital economy, and the traditional form of criminal interaction is replacing the traditional macro criminal networks, which are attended by visitors to forums, chat rooms, closed online communities. After all, to enter this segment you need to earn trust, have a certain status and reputation. It is no coincidence that the electronic environment greatly complicates the identification of the offender and contributes to the emergence of a new charac-

teristic feature of crime in the digital economy – many episodes of criminal activity.

It should be noted that, *in contrast to payments using traditional bank payment cards and Internet banking systems, payments by electronic means are often not personalized, which is an important criminological factor.* The fundamental question is under what conditions these economic relations can be transformed into criminal law. *Firstly,* the risk of becoming a victim of fraudsters who use anonymous proxy servers and twin sites to deceive and become inaccessible for identification is large enough. *Secondly,* given the transnational nature of electronic information exchange and a significant number of intermediaries between the source and addressee of information, the procedure for establishing the legal status and virtues of all participants in this process is complicated, and therefore the problem of criminal liability of Internet providers becomes relevant.

Considering the above, *China* introduced the radical methods in this format. Since February 2019, the government of the PRC cyberspace has obliged all owners of blockchain services to collect user identification data and freely transfer them to law enforcement agencies. The policy of the PRC in this direction provides for total control by the state. In 2018, China banned Initial coin offering (ICO), crypto exchanges, and a blockchain conference on related topics. Against this background, it is the state that actively invests in large blockchain projects. A support fund of blockchain projects has recently been established in the amount of 72 billion US dollars, which will operate in major cities of China.

In Switzerland, Canton Zug became a platform with a developed infrastructure for the adaptation and implementation of blockchain projects. This region even got the name «Crypto Valley», where banking institutions operating both with Fiat and cryptocurrencies are represented, there is a university for preparing blockchain specialists of HSLU-I, the headquarters of leading blockchain startups such as: «Ethereum», «Monetas», «Lykke». From 2014, pilot projects began to appear in the canton of Zug, which used the blockchain platform. Campaigns were launched to conduct referendums, electronic identification of citizens, accepting transfers of citizens for housing and utilities services, and transport.

The world community is closely monitoring the situation and trying to influence it. Thus, during 2016–2019, quite a few world forums took place, during which experts identified the 10 most acute international problems and risks for the world economy that are spread by organized crime, in particular, these are: financial crimes, including illegal taxation, financial security and the exchange of financial resources, investments and assets; production, storage, transportation and sale of counterfeit products; theft and unlawful use of intellectual property; illicit trafficking in weapons and means of destruction; illegal removal, storage, transportation and use of human organs for transplantation; online organized pedophilia and child pornography; illegal gambling and lottery businesses, including the creation of virtual casinos, illegal computer games that provide for unlicensed monetization etc.

The phenomenon of «corruption by organised crime» is the subject of increased attention from policymakers in the *United Kingdom of Great Britain and Northern Ireland.* This focus is notable, given the limited political and academic consideration of the scope and meaning of this intersecting term. Both «organised crime» and «corruption» are difficult notions to pin down, definitionally and empirically, and such complexity is compounded by their conjunction (Campbell, 2016).

For example, since *in most countries of the European Union,* as well as *in the United States,* cryptocurrency is not considered as a means of payment, but as a commodity, it is de facto legalized. The vast majority of participants in these and similar platforms are good citizens and has nothing to do with crime. However, the lack of detailed regulations and law enforcement practices makes such a business a «gray» zone, where the crime goes. *Europol experts* note that organized criminal groups that operate in the eurozone differ in their organizational structure, functionality and composition. In the EU, the phenomenon of activation of small high-tech criminal groups that operate in criminal online commodity markets is recorded. As a rule, in such groups professional criminals are a small number of individuals, and the main contingent consists of employees of IT companies, banking institutions, financial companies etc.

During the conference on the global use of cryptocurrency, held in January 2017 in Qatar, for the first time the question was raised about small high-tech groups, which in *the United States* are called «organizations-werewolves», and French law enforcement officers called them – «Mobius criminals». Some people mistakenly believe that such groups relate exclusively to cybercrime, because the spectrum of their criminal activities is quite wide. If earlier criminals used military or civilian technologies, adapting them for their needs, then in reality criminal groups themselves develop technologies, use them as a separate side business and realize through their interests in civil and military spheres. Modern criminals quickly adapt to technical innovations and create and implement technologies themselves. Adaptation options can be quite diverse.

Europol's greatest concern is the emergence of so-called «Mobius» criminal groups in the EU. Typical features of these groups are: small number, legal nature of activity, high level of their competence and professionalism. Such groups are created

by the order of large business structures outside the EU. The development of information and other high technologies affects the constant increase in the destructive potential of such small criminal groups. Over the past five years, small criminal groups have been able to harm not at the level of an individual business or a local community, but at the scale of megacities and large corporations.

At the end of 2018, realizing the scale of the spread of crime in cyberspace and having concern about the threatening trends of its spread, *the UN General Assembly* approved the resolution «On counteracting the use of information and communication technologies for criminal purposes». The European Union, in turn, has strengthened responsibility for crimes related to the blockchain and cryptocurrency. The reason for this decision was the massive proliferation of malicious programs that lure money from ordinary EU citizens.

Technological innovations are important factors affecting the activities, structure and *methods of organized «digital» crime in Europe.* European organized crime groups demonstrate a high degree of fitness and creativity in the use of new technologies. The Internet and its growing connectivity to all components of the physical environment are increasingly affecting the forms of serious organized crime. The «Internet things» sphere is also constantly expanding. The ability to connect all types of devices is becoming a reality for households and enterprises in the EU countries. Unlike traditional computers and tablets, smart phones and things connected to the Internet remain extremely vulnerable. In million cities in the EU, up to 90 % of the public Wi-Fi nodes are not protected by encryption. Accordingly, cybercriminals can connect to any of the millions of subscribers who use these nodes daily. According to Europol experts, the greatest threat in the field of organized crime in the coming years will be not artificial intelligence or big data, but transformations of extremely vulnerable to external malicious intrusion of smartphones, e-wallets and access points to numerous services and programs that require identification of personal data (Skuratovska, 2016). The analysis of the presented materials allows to determine the ways of countering organized crime in the digital economy, which are: victimological prophylaxis; technical anti-virus law enforcement support, which includes regular updates of licensed software, forensic technology; attracting new IT specialists to the departments of relevant law enforcement agencies; international digital integration, rationing on the legal basis of information exchange, coordination of the conceptual apparatus on the digital economy and its components; generalization and practical support of the dissemination of the best practices of European experience in countries with developed digital economies in the field of combating crime in this field; risk management of digital security in the economic sphere at the level of world integration, the state, individual industries, the private sector, enterprises of strategic importance to the state.

Conclusions

The digital economy in the EU states is developing progressively, primarily in such areas as: cloud technologies, Internet banking, and electronic services for the purchase of goods using a smartphone, block chain, online consultations and etc. Unfortunately, the existing regulatory framework at the EU level cannot provide an adequate level of resistance to technological and digital crimes. The European community is aware of all the risks and threats that cybercriminals can spread, but effective universal mechanisms of systemic struggle have not yet been developed. The general trend, which is stored in the EU in the format of intensifying criminal activity, is one step ahead of the law and practice of law enforcement in the «digital» space. Against this background, the number of crimes committed in the field of IT-technologies is constantly and dynamically growing. Annually criminals launder billions of euros using high-tech and, in particular, cryptocurrency, because government bodies have no influence on these processes, and the police are not able to monitor and block such transactions. Even if it is proved that the transaction is criminal in nature, law enforcement agencies are not able to freeze it or cancel it, unlike the traditional banking system, which requires the development of appropriate measures of mechanisms and their practical implementation.

Thus, law enforcement agencies and representatives of the digital economy industry should ensure parity principles of interaction and cooperation at both the operational and strategic levels. We can also confidently state that organized crime in the digital economy has a cross-border nature, and therefore measures to counter such crime include setting up, above all, effective international cooperation in this field.

Thus, currently, in the EU, there remains an expressive barrier between cybercrime and traditional organized crime groups, which is associated with different educational, cultural and professional levels of participants in these criminal organizations, as well as differences in ethnic and territorial composition, and the digital economy and its leading industries all remain vulnerable segments of the criminal encroachment.

REFERENCES

Campbell, L. (2016). "Corruption by Organized Crime" - A Matter of Definition? *Current Legal Problems, 69(1),* 115-141. doi: https://doi.org/10.1093/clp/cuw004.

European Cybercrime Centre - EC3. *Combating crime in a digital age.* Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia, Cyber security in Ukraine: legal and organizational issues: Proceedings of the All-Ukrainian Scientific and Practical Conference. (2016). (p. 233). Odesa: ODUVS [in Ukrainian].

Liashenko, V.I., & Vyshnevskyi, O.S. (2018). *Tsyfrova modernizatsiia ekonomiky Ukrainy yak mozhlyvist proryvnoho rozvytku [Digital modernization of the Ukrainian economy as an opportunity for break-through development].* Kyiv: NAN Ukrainy [in Ukrainian].

Skuratovska, D.V. (2016). Ways to improve management costs. *International scientific magazine "Internauca", 6.* doi: https://doi.org/10.21267/IN.2016.6.2294.

Stoica, O., & Ihnatov, I. (2016). Exchange rate regimes and external financial stability. *Economic Annals, 209(61),* 27-43. doi: https://doi.org/10.2298/ EKA1609027S.

YeS pratsiuie nad posylenniam borotby z vidmyvanniam hroshei-FT [The EU is working to strengthen the fight against money-laundering-FT]. *Ukrainski natsionalni novyny: informatsiine ahentstvo, Ukrainian National News: Information Agency.* Retrieved from https://www.unn.com.ua/uk/news/1751338-yes-pratsyuye-nad-posilennyam- borotbi-z-vidmivannyam-groshey-ft [in Ukrainian].

Стаття надійшла до редколегії 06.12.2018

Гребенюк М. В. **–** кандидат юридичних наук, доцент, керівник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, Київ;
ORCID: https://orcid.org/0000-0003-1249-5576;

Черняк А. М. **–** доктор юридичних наук, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, м. Київ;
ORCID: https://orcid.org/0000-0002-4958-783X

Європейський досвід протидії використанню організованою злочинністю провідних галузей цифрової економіки

Цифрова економіка в глобальних масштабах стрімко розвивається та є акселератором інновацій, конкурентоздатності й економічного зростання у світі. Більшість передових країн світу, таких як США, Канада, Японія, Німеччина, розвивають цифрову економіку й упроваджують цифрові технології у своїх суспільствах як стратегічну мету, що в перспективі має стати рушійною силою інноваційного розвитку, зокрема й для української економіки. ***Метою*** *статті є висвітлення європейського досвіду запобігання та протидії організованій злочинності у сфері цифрової економіки на підставі аналізу новел сучасного законодавства. Теоретичний базис і наукову проблематику обраного наукового напряму розглянуто у фундаментальних працях таких науковців, як В. М. Бутузов, М. О. Будаков, С. В. Демедюк, В. В. Марков, А. І. Марущак. Правоохоронні органи повинні володіти інструментами, методами й досвідом для протидії злочинним зловживанням методами шифрування й анонімізації. Для запобігання використанню злочинцями методів шифрування й анонімізації правоохоронні органи мають здійснити перепідготовку кадрів, причому не лише працівників тих підрозділів, що здійснюють боротьбу з кіберзлочинністю, а також мати в розпорядженні необхідні програмно-апаратні комплекси.* ***Висновки.*** *Основне завдання, на виконання якого спрямована цифрова економіка, – запровадження цифрових технологій у промислове виробництво, освіту, медицину й інші сфери. Сектори економіки, що використовують цифрові технології, розвиваються швидше та якісніше. Сфери життєдіяльності, зокрема освіта, медицина, транспорт, сільське господарство, що модернізуються завдяки цифровим технологіям, функціонують значно ефективніше та набувають нової цінності. Доцільно виокремити злочинність як категорію для вивчення саме у сфері цифрової економіки. Оцінка впливу цифрової економіки на національну та світову економіку засвідчує актуальність проблеми суцільної модернізації злочинності, яка постійно вдосконалюється в умовах активної електронізації та цифровізації суспільства. Ще один фактор, який слід ураховувати в процесі протидії злочинам у сфері «цифрової економіки», – це колосальна віктимність.*

Ключові слова: протидія; організована злочинність; цифрова економіка; європейський досвід; інновація; правоохоронні органи; віктимність.