Legal Horizons , № 4, 2023:
DOI: https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

Basic principles of combating cybercrime: international experience

Galyna Didkivska,
Doctor of Law, Professor,
professor of the Criminal Department
Law and Process of the
State University of Ukraine,
http://orcid.org/ 0000-0003-1714-4804

Dmytro Shevchenko,
Doctor of Law.
Professor of the Criminal Department
of Law and Process of the
State University of Ukraine,
http://orcid.org/0000-0002-7891-3331

Abstract. At the current stage of society's development, the importance of innovative processes taking place in our society in connection with global informatization is increasingly felt. But along with positive achievements, informatization is accompanied by side, negative phenomena of a criminogenic nature, which include computer crime. This, of course, requires the immediate creation of a system of combating this type of crime at the state level. For modern society (in the period of its transition from the industrial stage of development to the new one - post-industrial, informational), the relevance of this problem is beyond doubt. According to various expert estimates, worldwide losses from the activities of cybercriminals range from 300 to 800 billion euros annually. At the international level, a number of legal acts recognize that cybercrime threatens not only the national security of individual countries, but also the security of humanity and the international legal order.

For many countries, in particular for Ukraine, cybercrime is a fairly relevant phenomenon, generated by the widespread introduction of modern information and telecommunication technologies into economic processes.The characteristic features of crimes in the field of information and telecommunication technologies are: – the need for wide application of special knowledge in the detection and recording of crime traces in electronic form; – organization and cross-border nature (broad interregional and international connections); - high latency caused by the reluctance of the private sector to inform about such crimes due to distrust in the potential capabilities of law enforcement agencies and reluctance to admit weaknesses in their security systems; - a high level of technical support for offenders.

Keywords: criminal offenses, crime, cyberspace, crime, information and telecommunication technologies, prevention, counteraction, determinants, qualification problems.

Actuality of theme. The main problems of detection, disclosure and investigation of «cross-border» crimes using the global Internet network include the territorial distribution of crime traces and their storage for a short period of time. It is sometimes difficult for law enforcement officers to delineate the areas where modern crimes are committed. Criminals on the Internet have a high degree of anonymity, and the information stored in computer systems is of a short-term nature. Taking into account the peculiarities of crimes in the field of information and communication technologies, the interaction of the operative division of internal affairs at all levels is of great importance for the effectiveness of their operational documentation , including with representatives of law enforcement agencies of other countries (Korystin et al., 2012).

Analysis of recent research and publications. Current problems of protecting and protecting the cyberspace of European states at the legislative and institutional level were studied by the following foreign scientists: T. Wing Lo, Dina Siegel, Sharon I. Kwok, Martin Hrabalek, Marie Chene, Petrus C. Van Duyne, Nikos Passas, Gert Vermeulen and others . In view of the pan-European trends in the specified field, Ukrainian scientists subjected to a critical analysis the content and organizational and legal dimensions of the current problems and prospects of the protection and protection of the cyberspace of Ukraine in terms of combating cross-border crime. In particular, such specialists as A.V. Balendr, G.V. Didkivska, D.A. Kuprienko, Yu.B. Kurylyuk, A.M. Prytula, S.O. Filippov and others. At the same time, it is worth noting that most of the research was conducted in the period preceding the aggressive war of the Russian Federation against Ukraine.

DOI: https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

In view of the above, the purpose of the article is to highlight and analyze the strategic directions of European integration in the field of combating cybercrime, which relate to the system of protection and protection of the information and communication space, as a component of the formation of a pan-European security cyberspace.

Basic outline of the material. The strategy of state approaches and mechanisms for improving information systems should help reduce the scale of cybercrime and create the main principles of the national policy of countering cybercrime in international cyberspace. Anti-cybercrime in a broad sense includes nationwide measures of an economic, political, educational and other nature, as well as a set of special measures aimed at directly combating crime. Given the international nature of cybercrime, the harmonization of national laws is of vital importance in combating it. However, harmonization should take into account regional requirements and opportunities. The great importance of regional aspects in the implementation of strategies to combat cybercrime is emphasized by the fact that many legal and technical standards have been agreed between the countries of the world. The global cyber security program is based on five main principles: 1) legal measures; 2) technical and procedural measures; 3) organizational structures; 4) creating potential; 5) Current issues of combating cybercrime and human trafficking. international cooperation. It is clear that the Ukrainian system of state mechanisms for combating cybercrime must use all these principles. Among the five principles, when considering a cybercrime strategy, legal measures are probably the most important.First, these measures require the adoption of basic provisions of criminal law, which provide for criminal liability for such actions as computer fraud, illegal access, data distortion, copyright infringement, distribution of child pornography, etc. The mechanisms and tools needed to investigate cybercrimes can be significantly different from those used to investigate general crimes. In connection with the international scale of cybercrime, it is necessary to further refine the foundations of national legislation in order to have the possibility of joint cooperation with law enforcement agencies abroad. Effective fight against cybercrime requires a developed organizational structure. Without a properly created system of relevant bodies that avoids duplication and clearly distributes powers, one can hardly wait for a comprehensive solution to the legal, technical and social aspects of this problem. Cybercrime is a global phenomenon. In order to be able to effectively investigate cybercrimes, it is necessary not only to harmonize legislation, but also to develop appropriate mechanisms for international cooperation. The level of trust must increase not only between states, but also between the private and public sectors. One of the most important elements in cybercrime prevention is user education. Some cybercrimes, especially those involving spoofing scams, tend not to be due to a lack of technical protections, but to ignorance or simple irresponsibility.There are various software products that allow you to automatically identify some fraudulent websites, although unfortunately not all. Although technical protections will continue to evolve and available software products will be regularly updated, such products cannot yet replace other approaches. A user protection strategy based only on software products does not yet guarantee full user protection (Shvets, 2017).

In order to improve cooperation, the Convention provides for the creation by the parties at the national level of a body to make contacts 24 hours a day for the purpose of providing immediate assistance for the investigation or prosecution of criminal offenses related to computer systems and data, or for the purpose of gathering evidence in electronic form concerning criminal offence. Such assistance includes facilitating or, where permitted by domestic law and practice, directly: providing technical advice; preservation of data in accordance with articles 29 («Urgent preservation of stored data») and 30 («Urgent disclosure of stored data on the movement of information»); collecting evidence, providing legal information and establishing the whereabouts of suspects (Article 35) (Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems, 2003).

In a number of interstate regulatory legal acts (Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems, 2003; Convention, 2004; Convention on informational and legal cooperation concerning «Information public services», 2001) it is recognized that cybercrime today poses a threat not only to the national security of an individual state, but also threatens humanity as a whole. That is why this problem is given considerable attention in many states. Having analyzed the experience of the police of many countries of the world in the field of countering cybercrime, it should be noted that this direction is provided in such basic ways as assigning additional functions to existing police units or creating special units.The creation of special police

DOI: https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

units in the field of countering cybercrime is practiced in many countries of the world, in particular in Australia, Belgium, Belarus, Great Britain, Denmark, Estonia, India, Canada, Malaysia, the Netherlands, Germany, Norway, Poland, the USA, Switzerland, Sweden, etc. Among the main functions of these divisions, the following are distinguished:– monitoring of cyberspace in order to detect cybercrimes, viruses or malicious software;– implementation of operational search and intelligence measures in order to record the illegal activities of cybercriminals; investigation of cybercrimes, provision of methodical and practical assistance to other industry services and law enforcement agencies within their competence;– accumulation, summarization and analysis of information on cybercrime;– prevention of cybercrimes with the help of the public and mass media;– training of police officers. Some of the special units of the police in the field of combating cybercrime (or they are also called special units for combating crimes using information technologies) also perform additional functions: - detection of cybercrimes; - prevention and supervision of telecommunication services; - expert research of evidence on electronic media; – creation of an appropriate database on crimes in cyberspace and its constant updating; – provision of services to banks regarding the protection of personal information of clients, etc. For example, in India, cyber crime investigation units may hire professional hackers to solve them.It should be noted that during the investigation of cybercrimes, considerable attention is paid to assisting the victim in restoring damaged or lost information, all necessary measures are taken to preserve evidence in the case (Sen, 2014).

The problem of countering computer crime is a complex problem. Laws of Ukraine and other regulatory documents in the field of cyber security must correspond to the current level of information technology development. To this end, it is necessary to carry out purposeful work on the harmonization and improvement of the legislation regulating the dissemination of information in telecommunication networks. One of the priority directions is also the organization of interaction and coordination of efforts of law enforcement agencies, special services, the judicial system, providing them with the necessary material and technical base, as well as the development of public-private partnership (Shvets, 2017).

In addition, in recent years, various regions of the world have used a number of their own approaches to combat cybercrime. Thus, in 2002, the Commonwealth of Nations developed a model law on computer and computer-related crimes, the purpose of which is to improve the legislative norms of the member states of the Commonwealth in the field of combating cybercrime and to deepen international cooperation. In the absence of this agreement, for the development of cross-border cooperation in this field, the members of the Commonwealth of Nations would have to conclude a number of bilateral agreements among themselves, which would greatly complicate the cooperation procedure. The model law contains, in particular, provisions on international cooperation. Since it has a regional character, its provisions apply only to the member states of the Commonwealth (clause 20). The European Union has made efforts to harmonize the legislation on cybercrime, which operates on the territory of the member states of the organization.To this end, the following were adopted, in particular: Directive No. 2000/31/EC of the European Parliament and the Council on some legal aspects of information society services, such as electronic commerce in the domestic market; the framework decision of the Council of the European Union 2000/41/JHA on combating fraud and falsification of non-cash means of payment; framework decision of the Council of the European Union 204/68/JHA on combating sexual exploitation, etc. (paragraphs 20–21) (Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 2010). It should be noted that on the way to improving administrative and legal protection against cybercrime in Ukraine, we should study the positive experience of law enforcement agencies of other countries in this direction. In particular, one of the important areas of activity of the Canadian police is the fight against computer and telecommunication crimes, which are investigated by the Royal Canadian Mounted Police (Federal Police, RCMP) computer crime unit, relying on data from the Canadian Police Information Center and cooperating with other countries. The unit's activities are aimed at investigating and solving crimes related to computers and telecommunications. The information technology protection section ensures the protection of federal state computer centers, the private sector, provides consultations, and trains personnel to work on computer protection. Employees of the unit assist the police in conducting investigations of crimes involving computer systems.Given that the information system allows messages to be transferred from one terminal to another almost immediately, there are about 2,500 access points in Canada, which include about 1,285 federal and provincial police stations. 1180 subdivisions of specialized departments of the KKKP are

DOI: https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

connected to the system lines (Varunts, 2012).

Undoubtedly, this area of police activity is important, since the economic losses have already reached a wide scale, some criminals operate internationally as an organized group. At the same time, it should be recognized that Canadian legislation on the definition of computer crime needs improvement. Given that the tasks faced by the police units in the fight against computer crime are international in nature and not specific to Canada, they actively cooperate with other countries and Interpol in order to improve the legislation in this direction. Solving computer crimes is a difficult task, primarily due to the time factor. Because data transfers can be accomplished almost instantaneously, it is often futile to look for any evidence of a violation of international law. According to the CCCP, many computer crimes are committed by children under the age of twelve. According to the Criminal Code of Canada, in order to establish criminal liability, it is necessary to prove the unauthorized use of a computer system and the intention of the person to cause harm by his actions. Such an approach requires clearly establishing the parameters of access to computer equipment in order to prevent violations. It is necessary to take into account data about individuals, access parameters taking into account restrictions, the ability of employees to «experiment» with programs. Qualified advice on possible misconduct in this direction can be provided by the Ministry of Justice or the relevant unit of the CCCP.It should be noted that the method of investigating cases of unauthorized remote access to computer networks is technically complex, specialized police units deal with them. In view of the danger of computer crime, the trend of its development and impact on the world community, symposia on the prevention and cessation of computer crime are regularly held within the UN. As one of the directions, specialists note software methods of information protection in computer systems for collective use by improving the automatic control system. Actions and management of the fight against economic crimes are aimed at prevention and reduction of crimes related to the illegal use of telecommunication systems, both state and international. The Information Center helps police units. Police activities related to the prevention and disclosure of acts related to cybercrime are also aimed at the multifaceted development of relations with the largest possible social circle through mass media, consultative meetings with members of the public, relations with various authorities and management bodies, public organizations, and individual citizens. Thus, the police is an important partner in the community of agencies engaged in the fight against crime, including cybercrime, ensuring compliance with human rights, ensuring the protection of federal state computer centers, and the private sector (Varunts, 2012).

The effective fight against computer crime requires more effective and efficiently functioning cooperation of law enforcement agencies of different countries, including within Interpol. Taking into account the peculiarities of crimes in the field of information and communication technologies, the interaction of the operational division of internal affairs at all levels is of great importance for the effectiveness of their operational documentation: intra-departmental - with other operational divisions of the criminal police, research expert forensic centers and investigative units; intrastate - with other law enforcement agencies of Ukraine, labor collectives, public organizations and the population; international - with law enforcement agencies of other countries. Thus, the main types of cooperation of internal affairs bodies of Ukraine with law enforcement agencies of other states are:– exchange of operational and investigative information; - sending legal assistance in criminal cases; - departure of members of investigative and operative groups abroad for presence during the performance of investigative actions and operational-search activities; - departure for the exchange of information of an operational-but-search nature; - departure abroad for presence during investigative and other actions within the scope of providing legal aid;– departure for escorting wanted and detained persons abroad;– departure of employees of the border police of Ukraine, the Ministry of Internal Affairs and Communications of Ukraine to neighboring regions of neighboring states in operative and investigative cases;– arrival of law enforcement officers of foreign countries to Ukraine for investigative and operative investigative actions (Korystin et al., 2012).

The modern stage of the formation of civil society is determined by the entry of Ukraine into the leading technologically developed countries of the world, into the global information space. That is why we should use the experience of countries that already have quite serious developments in the field of ensuring information security (Lipkan, 2006), since it is an integral direction of building an information society, the development of which should go not only through increasing the technological capabilities of information security exchange, but also due to a deep awareness by all subjects of information relations - owners of information and its users, producers of

DOI: https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

information technologies and means, service providers, the state of the need to take all measures to protect information resources and ensure the security of the state, including taking into account the foreign experience of countermeasures cybercrime in the field of administrative and legal support.

An important role is also played by unquestioning compliance with established information security rules and procedures. For example, if users know that their financial institutions will never contact them via email asking for their password or bank account details, they will not become victims of phishing or identity theft attacks. Educating Internet users reduces the number of potential victims of cyber incidents. The state should develop an appropriate informational program of reasonable behavior regarding the prevention of cybercrime.Public campaigns, schools, information centers and universities should be involved in its dissemination, implementing private-state partnerships (Shvets, 2017).

Conclusion. So, as we can see, only by the coordinated efforts of organizations and departments, regardless of the forms of ownership, by establishing international cooperation, using modern information protection technologies, it is possible to get the benefits not only of electronic business, but also of the information revolution as a whole, not forgetting the information security of the state and individual citizens . It should be noted that the improvement of legal protection against cybercrime in Ukraine should take place taking into account the national cultural-historical, socio-economic features of the country on the basis of a detailed scientific analysis of international legislation and the experience of other countries in the field of combating cybercrime with the aim of optimal entry into the European and world legal system get together.

References:

Additional Protocol to the Convention on Cybercrime, which concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems. (2003). Retrieved from: http://zakon.rada.gov.ua/laws/show/994_687

Convention (2004). Retrieved from: http://zakon.rada.gov.ua/laws/show/995_789.

Convention on cybercrime (2007) No. 65., Art. 25-35

Convention on informational and legal cooperation concerning «Information public services»: (2001). Retrieved from: http://zakon.rada.gov.ua/laws/show/994_559

Korystin O. E., Butuzov V. M., Vasylevich V. V. and others (2012). Combating cybercrime in Ukraine: legal and organizational principles: training. manual

Lipkan, V. A. (2006) Information security of Ukraine in the conditions of European integration: training. manual

Sen, R. Yu. (2014). The experience of foreign countries in the field of cybercrime investigation. Ministry of Internal Affairs of Ukraine, Kharkiv. national University of Internal Affairs affairs -Kharkiv: Human Rights

Shvets, D. V. (2017). State mechanisms for fighting cybercrime. Retrieved from: https://univd.edu.ua/general/publishing/konf/15_11_2017/pdf/22.pdf

Twelfth United Nations Congress on Crime Prevention and Criminal Justice (2010). Retrieved from: http://www.un.org/ru/conf/crimecongress2010/

Varunts, L. D. (2012) Experience in the organization of the activities of the Royal Canadian Mounted Police and ways of its use in Ukraine