Заслуженого деятеля науки и техники Украины, доктора юрид. наук, проф. Е.Л. Стрельцова. – Х. : ООО «Одиссей», 2002.
10. Хавронюк М.І. Злочини проти основ національної безпеки України / М.І. Хавронюк // Кримінальне право України. Особлива частина: підручник (Ю.В. Александров, О.О. Дудоров, В.А. Клименко та ін.) / За ред. М.І. Мельника, В.А. Клименка. – К. : Юридична думка, 2004.
11. Хавронюк М.І. Злочини проти основ національної безпеки / М.І. Хавронюк // Науково-практичний коментар Кримінального кодексу України від 8 квітня 2001 р. / За ред. М.І. Мельника, М.І. Хавронюка. – К. : Канон, 2001. – (1104 с.).

SAMOILENKO O. A.

National University «Odesa Law Academy»,
Associate Professor of the Department of Criminalistics, PhD in Law

ISSUES OF IMPLEMENTATION IN THE INTERNAL LEGISLATION OF UKRAINE NORMS OF INTERNATIONAL LAW IN THE SPHERE OF FIGHTING CRIMES TAKEN IN CYBERSPACE

The article deals with the implementation of the norms of international law in Ukraine's internal legislation, in particular the Council of Europe Conventions regarding the criminalization of crimes committed in cyberspace.

Key words: *implementation cyberspace, cybercrime, convention, criminalization, crime.*

Despite the detailed description at the interregional level of specific cybercrime compositions, the nature and list of offenses related to the cyberspace situation in national legal systems differ. Ukraine is no exception.

The starting points for understanding the legal framework of Ukraine in the fight against crimes committed in cyberspace are the norms adopted by European states in the city of Budapest on November 23, 2001 of the Council of Europe Convention on Cybercrime. Ukraine joined it with reservations by ratification on September 7, 2005. Today we can talk about other numerous agreements, universal, regional and local treaties on combating crimes in cyberspace, the norms of which can be implemented in the domestic legislation of Ukraine.

The standards of some of these treaties are directly recognized in the Convention on Cybercrime itself. In particular, the text of the Convention refers to such international acts ratified by Ukraine:

– in part of the determination by the state of boundaries of the observance of the human right to information, is an integral element of the human right to freedom of speech, – Council of Europe Convention on the Protection of Human Rights and Fundamental Freedoms of 1950 and the UN International Covenant on Civil and Political Rights of 1966;

– in terms of ensuring the protection of personal data stored in data files for automated processing, and preventing unauthorized access, modification or distribution – the Council of Europe Convention on the Protection of Persons in Connection with the Automated Processing of Personal Data of 1981;

– in terms of ensuring the protection of the child from all forms of sexual exploitation and sexual abuse – the UN Convention on the Rights of the Child 1989, the International Labor Organization Convention on the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labor;

– in terms of mutual assistance requests transmitted by telecommunication routes – to the European Convention on mutual assistance in criminal matters; – with regard to the protection of intellectual rights – to the Bern Convention for the Protection of Literary and Artistic Works (Paris Act of July 24, 1971, amended on October 2, 1979), Agreement on Trade-Related Aspects of Intellectual Property Rights; World Intellectual Property Organization Agreement on Copyright under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention);

– in terms of ensuring the equality of people before the law and equal protection against all discrimination and against all incitement to discrimination – to the International Convention on the Elimination of All Forms of Racial Discrimination;

Consider individual issues of implementation of the norms of international law in the national legislation of Ukraine regarding the criminalization of crimes committed in cyberspace.

The United Nations Convention against Transnational Organized Crime recommends that states criminalize crimes against the principles of sovereign equality and territorial integrity of states, as well as the principle of non-interference in the internal affairs of other states, laundering of proceeds of crime, participation in an organized criminal group, corruption, obstruction of justice conditions: 1) in more than one state; 2) in one state, but the essential stage of preparation, planning, management or control occurs in another state; 3) in one state, but with the participation of an organized criminal group that carries out criminal activities in more than one state; 4) in one state, but significant consequences occur in another state. Paragraph 29 of this Convention refers to training programs for law enforcement personnel in the aspect of «the methods used in the fight against transnational organized crime, which are committed using computers, telecommunications networks and other types of modern technologies».

For example, with the advent of cryptographic currency technology, the creation and circulation of which is based on the methods of cryptographic protection of information, corrupt practices, laundering of proceeds of crime through the use of such mutual settlements have become elusive for law enforcement agencies. Indeed, in the process of turnover of such currencies, there is no single leading entity; this technology allows storing information about the currency turnover is divided – on computers all over the world [1].

This is just one example of the opportunities that cyberspace provides for the commission of these crimes. At the same time, there is no indication in the national criminal law that cyberspace technologies are used for making public appeals or distributing materials calling for encroachment on the territorial integrity and inviolability of the state; financing actions committed to forcibly change or overthrow the constitutional system or seize state power, change the borders of a territory or state border; high treason; sabotage; espionage; legalization of proceeds from crime and other transnational organized types of criminal offenses.

Also noteworthy is the issue of regulation of criminal responsibility for the use of cyberspace for the commission of a terrorist act and other crimes related to it. In Ukraine, this area of the fight against terrorism is affected by bilateral treaties concluded with the United States, the Republic of Slovenia, Montenegro, the Kingdom of Belgium, the Kingdom of the Netherlands. The problems of fighting cyber-terrorism in the international legislative field are reflected in the form of draft acts or local, bilateral international treaties on procedural law. The countries of the European Union are discussing an interregional project Clean IT, the purpose of which is to organize a rapid response in the event of a threat of an act of cyber terrorism [2]. However, since there is no corresponding universal international act, cyberterrorism as a phenomenon and methods of countering it in Ukraine remains the only subject of research by scientists (V. Butuzova, S. Gavrisha, S. Gnatyuk, V. Golubeva, D. Dubova, A. Korchenko, V. Lipkana, V. Shelomentseva, S. Hildret).

A similar problem concerns not regulated in Ukraine as the crime of theft, transfer and use of personal data. Some countries identify crimes of this type as an independent category, others believe that these actions fall under several articles of criminal law [3]. According to K.S. Shakhbazyan, the dissemination of information by computer networks can result in both massive violations of human rights (for example, propaganda of genocide, dissemination of the idea of racial inequality), and disrespect for the rights of individuals. Therefore, the dissemination of information by computer networks, causes massive violations of human rights, is considered as an international crime, which entails the emergence of international legal responsibility of states and individuals [4, p. 71]. In the criminal law sphere of Ukraine, this issue is highly relevant and not developed.

Thus, the continuous development of scientific and technical potential, the improvement of international cyber security legislation naturally leads to the need to supplement certain articles of the Criminal Code of Ukraine with a qualifying attribute regarding the use of the cyberspace environment to commit the corresponding types of crimes (Art. 109-114, 157, 158, 159 , 159-1, 185, 189, 191, 258, 258-2, 258-3, 258-5, 263, 359 of the Ukrainian Criminal Law).

References:

1. Mashchenko P. L., Pilipenko M. O. Technology Blockchain and its practical application. Science, technology, education. 2017. № 32. P. 61-64.
2. Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications. 2012. 21 sep. URL: https://edri.org/cleanit/

3. Independent Association of Ukrainian Banks «Anti-Kiber»: Cybercrime: Challenges and Forecasts. URL: http://anticyber.com.ua/article_detail.php?id=140.
4. Shahbazyan K. S. International legal bases of regulation of relations in the Internet: dissertations. lawyer Sciences: 12.00.11. Kiev, 2009. 222 p.

TARASENKO L. L.

Ivan Franko National University of Lviv,
Associate Professor at the Department of Intellectual Property,
Informative and Corporate Law, PhD in Law

DOMAIN NAME DISPUTES

Key words: *domain name, court, trade mark, intelectual property, web-site.*

The development of the digital environment leads to a large number of websites. Some websites are very popular among users and that promotes the company-holder of the website, its commercial name and activity results within the market. Every website has its own «name» posted in the Internet. This is the domain name (domain) identifying a web resource in the global information network.

At a time when practically every member of society has access to the Internet using a computer, phone, tablet or other device, the existence and operation of a website becomes a necessity for every company wants to present itself in the Internet-environment. Thereby, there are unfair competition signs through the using of a domain name (website name) closer to the domain name of the competitor (other entity). Thus, due to the mixing of two websites names for the Internet users-potential customers, a domain dispute between two domain holders of similar domain names emerges. There is no regulation under Ukrainian legislation of the procedure for settling domain disputes. There is no unified legal regulation of settling such disputes in the EU and in the world at large. This is due the fact that the Internet is «a space without borders» and the administration of the Internet address space is performing by NGOs guided by their own rules and principles.

Domain dispute is a dispute concerning the legality (unfairness) of the domain name registration and use between the holder of the domain name and other interested person (for example, trademark certificate holder). There is a point of view highlighted in scientific literature that the settling of disputes, regarding to domain names, usually requires special knowledge in the province of information technology that causes a great difficulty both to the parties to a dispute and to mediators trying to settle [1]. Such a position is rather controversial, since even the court (other entitled person or body), solving this category of cases, does not require an expertise to verify claims or objections. We consider that special knowledge (expertise) regards the