UDC 343.3+004

SAZANOVA Larysa Serhiivna,
senior lecturer of the department of foreign languages of faculty No. 4
Kharkiv National University of Internal Affairs
https://orcid.org/0000-0002-3722-2593;

KOTELEVETS Alina Vadymivna,
a fourth-year cadet of faculty No. 4
Kharkiv National University of Internal Affairs
https://orcid.org/0009-0003-2534-5638

SOME ASPECTS OF COMBATING CYBERCRIMES IN UKRAINE

Several issues in the field of combating cybercrime require special attention at the stage of the development of social, cultural and economic relations in Ukraine. Crime in a certain area is growing not only quantitatively. Such crimes are becoming more and more complex, the level of their antisocial orientation is increasing. This type of crime harms not only the economy of the country, but also the state order. The spread of computer crime led to the need to study this phenomenon, develop recommendations with the main directions of countering cybercrime.

Before moving on to the aspects of countering cybercrimes, it is important to note that there is still a debate about the definition of the concept and signs of cybercrimes and cybercrime in the science of criminal law and criminology, because at the national level this concept does not have a normative regulation (at the level of its legislative definition), however this term is used in Convention on Cybercrime known as the Budapest Convention on Cybercrime, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations [1]. Regarding scientific approaches to the definition of the concepts of “cybercrime” and “cybercrimes”, it should be explained that some scientists associate them with a specific object of crime (a computer, computer equipment or computer data and a method of committing a crime). The above-mentioned items are used for “committing a crime (crimes)” [2, p. 338] or a certain place of its commission “cyberspace” [3, p. 17], “virtual space” [4, p. 173]. Such approaches are somewhat simplistic, because if a computer is recognized as an object of crime, then any use of it, for example to cause bodily harm, will constitute a cybercrime. Regarding the connection of cybercrimes and cybercrime only with a certain space of committing a crime (crimes), one should refer to the research conducted by O. V. Manzhai.

Having analyzed the existing definitions of cyberspace, the scientist concluded that “cyberspace” is identified as a certain space. It is information environment space that exists with the help of technical computer systems during the interaction of people with each other, the interaction of technical computer systems and human management of these technical computer) systems [5, p. 216], which does not actually cover local networks (not connected to the Internet), let alone local computers.

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. "Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed" [1, p.7].

Ukrainian scientists identify factors that have a negative impact on the process of investigating computer crimes and need to be resolved as soon as possible:

– imperfection of criminal procedural legislation;

– an extremely weak regulatory framework designed to regulate the legal status and specific features of information resources;

– lack of methods for investigating crimes of the specified type;

– lack of generalizations of investigative and judicial practice;

– lack of a basic expert forensic center for the production of the necessary examinations of computer equipment;

– lack of methods for conducting forensic software and technical examinations.

The most effective measures directly aimed at countering cybercrime are the following: increasing the number of scheduled and unscheduled inspections; establishment of strict control over the circulation of technical means prohibited or restricted in free civilian circulation; adopting the experience of law enforcement agencies of other countries in this area; cooperation with the relevant bodies of other countries regarding the disclosure, investigation and prevention of crimes in the analyzed area, exchange of law enforcement experience; identification of persons prone to committing crimes in the analyzed area, etc. These measures require further scientific research developments to create effective tools for countering modern cybercrime challenges.

References

1. Convention on Cybercrime Budapest 23.11.2001. URL: https://rm.coe.int/1680081561

2. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : зб. наук. пр. Київ : Вид.- поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338–342.

3. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». Інформаційна безпека людини, суспільства, держави. 2010. № 1 (3). С. 16–18.

4. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172–177.

5. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. Право і Безпека. 2009. № 4. С. 215–219. URL: http://nbuv.gov.ua/UJRN/Pib_2009_4_50.

Received 15.04.2023