

РОЗДІЛ 1.

ІНСТИТУЦІЙНІ ТА ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Dykyi Oleh Viktorovich

National University «Odessa Law Academy»,
Dean of the Faculty of Cybersecurity and Information Technologies,
PhD in Law, docent

MECHANISM OF COUNTERACTION TO CYBERCRIME: CRIMINOLOGICAL ASPECTS

The twentieth century has become an era of new challenges, associated with the rapid development of science and technology, the emergence of new technologies. However, at the same time, socially-negative phenomena began to appear as positive practices, and cyber-security became one of them. Without going into the history of the emergence of cybercrime, it is worth noting that countering this phenomenon is extremely difficult through the constant emergence and development of existing technologies. In fact, law enforcement agencies are limited by law and technology, and criminals are deprived of such restrictions. In this regard, countering cybercrime is reduced to the investigation and suppression of criminal activity, in exceptional cases it is aimed at its prevention.

Given the current trends of cybercrime in the world, the UN General Assembly, in a resolution of 12/17/2018, expressed concern about the increase in cybercrime and the introduction of information and telecommunication technologies in the commission of many types of crimes. In this regard, recommended the Member States to intensify their efforts in the fight against cybercrime and the criminal use of information and communication technologies in all its forms and to develop international cooperation in this area, including the exchange of electronic evidence [1].

Usually, for effective counteraction to crime, including cyber-crime, the means and methods that are developed on the basis of modern scientific achievements are key. We believe that it is precisely criminological science that has such potential, since the subject of research includes crime itself and its determination, the personality of the criminal. On the basis of these components, it can develop effective means and methods of combating crime. It is criminological science that has the methodological apparatus that allows us to consider the problem of combating cybercrime in a comprehensive manner and propose ways to improve such activity. Now cybercriminology is at the stage of its formation – as a separate area of criminological science.

It is worth noting that the scientific support of countering cyber-crime, both in domestic and world science, is underdeveloped, despite numerous studies by scientists. There may be many reasons for this, for example, the lack of clear boundaries of the research subject, outdated methods of collecting and analyzing empirical material, ignoring the results of research in related industries, including technical, and the like. In this regard, the nature of cyber-crime is distorted, simplified to computer crimes or in the field of information technology. Moreover, the lack of deep criminological research on cyber-media creates real problems in the practice of countering this type of crime in the context of international cooperation. Thus, in the report on the work of the twenty-fifth session of the Commission on Crime Prevention and Criminal Justice of the UN Economic and Social Council for 2016, the importance of having adequate national legislation and enhancing international cooperation in the fight against cybercrime was emphasized. Also, there were different opinions on the best approach to fighting cybercrime at the international level [2]. For example, participants drew attention to the need to develop a new comprehensive international legal instrument on cybercrime, which would focus on, inter alia, procedural issues. Despite the fact that this issue is still unresolved, the main international document is the Convention on Cybercrime of

the Council of Europe, which was adopted in 2001. This indicates the absence of a unified approach to combating cybercrime, despite the formal definition of the mechanism for combating this type of crime and its components. Therefore, it is fundamental to determine the effectiveness of this mechanism in dynamics, in order to find the best practices in countering cybercrime.

List of sources used

1. Укрепление программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в особенности ее потенциала в сфере технического сотрудничества. Принята резолюцией 73/186 Генеральной Ассамблеи ООН от 17 декабря 2018 года. *Организация Объединенных Наций : офіційний веб-сайт*. URL: <https://undocs.org/pdf?symbol=ru/A/RES/73/186>

2. Доклад о работе двадцать пятой сессии (11 декабря 2015 года и 23-27 мая 2016 года) Комиссии по предупреждению преступности и уголовному правосудию Экономического и Социального Совета ООН. *Организация Объединенных Наций : офіційний веб-сайт*. URL: <https://undocs.org/pdf?symbol=ru/E/2016/30>

Key words: cybercrime, mechanism, counteraction

Ключевые слова: киберпреступность, механизм, противодействие

Ключові слова: кіберзлочинність, механізм, протидія