DYKYI OLEH

National University "Odesa Law Academy",
Dean of the faculty of cybersecurity and information technology,
PhD in Law, Docent

MODERN METHODOLOGICAL APPROACHES TO THE STUDY OF CYBERCRIME

The XIX – XXI century was the era of total informatization and the cyberization of all walks of life in most countries of the world. On the one hand, it made it possible to improve, simplify people's lives, and on the other, it created new challenges, such as cybercrime.

In recent years, cybercrime has grown at an alarming rate not only in Ukraine but in the world. This is due both to the lack of proper international cooperation and the rapid processes that take place in the cyber environment. Technologies change every year, new data systems and software are used by criminals. Of course, this requires adequate measures to respond to and prevent threats, which must be based on scientific and practical recommendations.

Because of current trends, the General Assembly of the United Nations in its resolution of 17 December 2018 expressed concern about the increase in cybercrime and the use of information and telecommunication technologies in the commission of many types of crimes. In this regard, it recommended that the Member States step up their efforts to combat cybercrime and use information and communication technologies in all its forms and to develop international cooperation in this area, including the exchange of electronic evidence [1].

Equally important is the scientific support for counteracting cybercrime, which is not sufficiently developed in domestic doctrine, despite applied research by scientists. There may be many reasons for this, for example, the lack of clear boundaries of the subject of study, outdated methods of collecting and analyzing empirical material, ignoring the research findings used, especially from developed countries in Europe and the USA, etc. In this regard, the nature of cybercrime is distorted, simplified to computer crimes or in information technology. Moreover, the lack of sound criminological research on cyber-media creates real problems in the practice of counteracting this type of crime in the context of international cooperation. For example, the report of the twenty-fifth session of the Crime and Criminal Justice Commission of the United Nations Economic and Social Council for 2016 emphasized the importance of adequate national legislation and enhanced international cooperation in the fight against cybercrime. They also expressed differing opinions on the best approach to combating cybercrime at the international level [4]. For example, participants drew attention to the need to develop a new comprehensive international legal instrument on cybercrime that would focus on procedural issues in particular. However, this issue has not yet been resolved, but the Council of Europe's Convention on Cybercrime, adopted in 2001, is the main international document.

For the first time, cyber criminology as a scientific field was proposed in 2007 by Indian scientist K. Jaishankar. In his work, the scientist defines the definition of cyber criminology: "... like, the doctrine of cause and effect in the commission of crimes that occur in cyberspace and their impact on physical space" [2]. Of course, this definition reflects the essence of criminology in General, and clerking as its component, and therefore requires further research through the prism of modern research.

In domestic scientific opinion, the term «cyber criminology» is almost never used. There are only descriptive references in Russian academic writings, such as: "At the intersection of computer science and criminology there is a new scientific direction cyber criminology. To date, cyber criminology is a private criminological theory that studies crime in cyberspace (cybercrime), its causes, personality traits, and measures to counter this phenomenon" [3].

Cyber criminology is clearly a multidisciplinary field of research. It covers forensics, sociology, psychology, victimology computer and internet science. In addition, the basis of cyber criminology is the study of criminal behavior and victimization in cyberspace from a behavioral theoretical point of view, which seems promising on the one hand, and super complicated on the other. This is primarily due to the empirical material. It is quite easy for scientists and practitioners to identify victims of cybercrime, but not criminals, and the available criminal case studies form an idea not of a professional cyber-criminal but of an amateur or a novice. This is one of the important problems that cyber criminologists need to address in order to develop effective measures to counter this type of crime. It is cyber criminology that should become the field of knowledge that will allow studying cyberspace in more detail in terms of violation of criminal law.

References:

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. Jaishankar K. Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*. 1(1). P. 1–6.
3. Шестаков Д.А., Дикаев С.У., Данилов А.П. Летопись Санкт-Петербургского международного криминологического клуба. Год 2014 // Криминология: вчера, сегодня, завтра. – 2015. – № 1 (36). – С.73
4. 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

Ключові слова: кіберкримінологія, кіберпростір, кіберзлочини.
Ключевые слова: киберкримология, киберпростир, киберзлочини.
Key words: cyber criminology, cyber space, cybercrime.