5. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems within the territory of the Union (Journal of Laws of the EU 2016 No. 194)

6. Szyszko A., Department of Safety and Crisis Management, Ministry of Energy, Meeting of the LTE working group

Ключові слова: кібербезпека, 5G Toolbox, інцидент, критична інфраструктура, сертифікація

Ключевые слова: кибербезопасность, 5G Toolbox, инцидент, критическая инфраструктура, сертификация

Keywords: cybersecurity, 5G Toolbox, incident, critical infrastructure, certification

Dykyi Oleh Viktorovych

National University «Odesa Law Academy»,

Dean of the Faculty of Cybersecurity and Information Technologies, Candidate of Law, Associate Professor

MODERN METHODOLOGICAL APPROACHES TO THE STUDY OF CYBER CRIMES

The XIX century was an era of total informatization and cybernation of all spheres of life in most countries. On the one hand, it has improved and simplified people's lives, and on the other, it has created new challenges, such as cybercrime.

In recent years, cybercrime has reached alarming proportions not only in Ukraine but in the world. This is largely due to the lack of proper international cooperation and the rapid processes that are taking place in the cyber environment. Every year, technologies change, new data systems are created, new software is used by criminals,

and so on. Of course, this requires adequate measures to respond to and prevent threats, which should be based on scientific and practical recommendations.

Given current trends, the United Nations General Assembly, in its resolution of 17 December 2018, expressed concern over the increase in cybercrime and the use of information and telecommunications technologies in the commission of many types of crime. In this regard, it recommended that Member States intensify their efforts to combat cybercrime and the criminal use of information and communication technologies in all its forms and to develop international cooperation in this field, including the exchange of electronic evidence [1].

No less important is the scientific support of combating cybercrime, which in the domestic doctrine is not sufficiently developed, despite the applied research of scientists. There can be many reasons for this, for example, the lack of clear boundaries of the subject of research, outdated methods of collecting and analyzing empirical material, ignoring the use of research results of scientists, especially from developed countries in Europe and the United States and more. As a result, the nature of cybercrime is distorted, simplified to cybercrime or in the field of information technology. Moreover, the lack of thorough criminological research on the cyber environment creates real problems in the practice of combating this type of crime in the context of international cooperation. Thus, the report on the twenty-fifth session of the Commission on Crime Prevention and Criminal Justice of the UN Economic and Social Council for 2016 stressed the importance of having adequate national legislation and intensifying international cooperation in the fight against cybercrime. Also, different opinions were expressed about 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, which will focus on, in particular, procedural issues. However, this issue is still unresolved, and the main international document is the Council of Europe Convention on Cybercrime, adopted in 2001.

Cyber criminology was first proposed as a scientific field in 2007 by Indian scientist K. Jaishankar. In his work, the scientist defines the definition of cyber criminology: «as the doctrine of causation in the commission of crimes occurring in

cyberspace and their impact on physical space» [2]. Of course, this definition does not reflect the essence of criminology in general and cyber criminology as its component, and therefore requires additional research through the prism of modern research.

In domestic scientific opinion, the term «cyber criminology» is almost non-existent. There are only descriptive mentions in Russian works, such as: «At the junction of computer science and criminology, a new scientific field of cyber criminology has appeared. Today, cyber criminology is a private criminological theory that studies crime in cyberspace (cybercrime), its causes, personality traits of cybercriminals and measures to combat this phenomenon» [3].

Obviously, cyber criminology is by nature a multidisciplinary field of study. It covers criminology, sociology, psychology, victimology, computer and Internet sciences. In addition, cyber criminology is based on the study of criminal behavior and victimization in cyberspace from a behavioral theoretical point of view, which on the one hand seems promising, on the other - extremely complex. This is primarily due to the empirical material. Thus, it is quite easy for scientists and practitioners to identify victims of cybercrime, but not criminals, and the available studies on the basis of convictions in criminal cases form an idea not of a professional cybercrime, but of an amateur or beginner. This is one of the important problems that cyber criminology needs to address in order to develop effective measures to combat this type of crime. It is cyber criminology that should become the field of knowledge that will allow a more detailed study of cyberspace 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.

Keywords: cyber criminology, cyber space, cybercrime.

Чанышев Рашид Ибрагимович

Национальный университет «Одесская юридическая академия», доцент кафедры информационных технологий, кандидат юридических наук, доцент

О НЕОБХОДИМОСТИ КОМПЛЕКСНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НОВЫМ ПРОФЕССИЯМ, СВЯЗАННЫМ С ЗАЩИТОЙ ИНФОРМАЦИИ

В последнее время во всем мире отмечается резкий рост числа инцидентов, связанных с информационной безопасностью. С учетом растущей цифровизации практически всех сфер жизнедеятельности человечества, эти угрозы стали представлять непосредственную опасность для жизни и здоровья людей [1].

Так, 4 октября 2021 года у пользователей ряда социальных сетей начались проблемы с доступом к Facebook, Instagram и WhatsApp. Неожиданным следствием этой проблемы стало то, что сотрудники компании Facebook не смогли попасть в собственный офис, а множество обычных пользователей не