***O. Kapitonova**, BA student*
***N. Boholiub**, PhD in Ped.*
Berdychiv Applied College of Industry, Economics and Law

CYBERCRIME AND JURISDICTION: ADDRESSING THE CHALLENGES OF TRANSNATIONAL OFFENSES

The rapid development of information technologies has led to the emergence of a distinct category of crime cybercrime. Due to its inherently transnational nature, cybercrime poses significant challenges to traditional legal systems, as offenders, victims, and digital infrastructure may simultaneously be located in different jurisdictions [5]. This creates substantial difficulties in determining applicable law and ensuring effective enforcement.

Cybercrime occupies a prominent place among transnational offenses, as it causes considerable economic and social harm and evolves alongside technological progress. Modern cybercriminals actively use anonymization tools, cryptocurrencies, and automated systems, which significantly complicates their identification and prosecution.

At the international level, efforts to combat cybercrime are based on a number of legal instruments regulating cooperation in cyberspace. These include the Council of Europe Convention on Cybercrime (Budapest Convention), the United Nations Convention against Transnational Organized Crime, and other international initiatives aimed at strengthening global cybersecurity [3, 4]. However, not all states are parties to these agreements, which creates regulatory gaps and weakens the effectiveness of international cooperation. Divergences between national legal frameworks further complicate cross-border investigations and prosecution [5].

Cybercrime is characterized by several specific features, including extraterritoriality, technological dependence, and rapid transformation into new forms. These characteristics significantly hinder the processes of evidence collection, investigation, and jurisdictional determination. In particular, conflicts of jurisdiction arise when multiple states claim authority over the same offense, leading to delays and legal uncertainty.

According to the Budapest Convention, cybercrimes can be classified into four main categories: offenses against the confidentiality, integrity, and availability of computer data and systems; computer-related offenses; content-related offenses; and copyright-related violations. This classification provides a unified framework for the legal qualification of cyber offenses at the international level.

A critical issue in combating cybercrime is the collection and admissibility of electronic evidence. Digital evidence, such as login data or cloud-stored information, is highly volatile and can be easily altered, deleted, or concealed. These challenges are exacerbated in cross-border contexts, where access to evidence depends on international cooperation mechanisms that are often slow and inefficient [2].

Furthermore, cybercriminal activities are increasingly organized, with groups operating across multiple jurisdictions and distributing their operations geographically to avoid detection and liability. This trend necessitates enhanced international coordination, including the development of joint investigative teams, rapid

information-sharing mechanisms, and advanced tools for monitoring financial transactions, particularly those involving cryptocurrencies.

From an analytical perspective, the current international legal framework remains fragmented and insufficiently effective in addressing the complexities of transnational cybercrime. While existing conventions provide a foundation for cooperation, their implementation is uneven, and enforcement mechanisms remain limited [1].

In conclusion, addressing cybercrime requires a comprehensive and coordinated international approach. The development of a universal legal instrument could significantly enhance global cooperation in this field. For Ukraine, a key priority is not only participation in international conventions but also the effective implementation of their provisions into national legislation and law enforcement practice.

REFERENCES

1. Аніщук В. В. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз / В. В. Аніщук, С. Г. Зицик // Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Випуск 83: частина 3. С. 19-23. – Режим доступу: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf
2. Гуцалюк М. Імплементація європейських стандартів у боротьбі з кіберзлочинністю: проблеми правового регулювання електронних доказів в Україні / Михайло Гуцалюк // Слово національної школи суддів України. 2024. №2(51): С. 167-176. – Режим доступу: https://slovo.nsj.gov.ua/images/pdf/2025_2_51/nsj02-51-2025.pdf
3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : міжнародний документ від 15.11.2000 р. // Верховна Рада України. Законодавство України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_789#Text
4. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 р. // Верховна Рада України. Законодавство України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text
5. Попко В. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі / В. В. Попко, Є. В. Попко // Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Вип. 66. С. 276-283. – Режим доступу: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/11/49.pdf