Section name – jurisprudence

CYBERCRIME AS A GLOBAL LEGAL PROBLEM

Remmelh Arina Andriivna
3rd year student
Kryvyi Rih Professional Law
College of the National University
"Odesa Law Academy", Ukraine
arinaremmelg@gmail.com
Scientific supervisor:
Bohatyrova Maryna Oleksandrivna
a teacher-methodologist
Kryvyi Rih Professional Law
College of the National University
"Odesa Law Academy", Ukraine
bogatyrevamarina342@gmail.com

Abstract: This article examines the problem of cybercrime in modern society. Special attention is paid to the legal regulation of cybercrime and the mechanisms for combating it. The study analyzes the main types of cybercrime and their impact on international security.

Keywords: cybercrime, criminal law, cybersecurity, international law, cyber legislation, cyber policy.

Introduction: Cybercrime has become one of the most serious challenges of modern society. The rapid development of information technologies and the widespread use of the Internet have created new opportunities not only for communication and business but also for criminal activity. Today criminals actively use digital technologies to commit fraud, steal personal data, and conduct illegal financial operations.

Purpose and objectives of the research: The purpose of this research is to analyze the problem of cybercrime in modern society and to examine the legal mechanisms used to combat such crimes. In order to achieve this goal, the study considers the concept of cybercrime, analyzes the most common types of cybercrime, and examines the legal regulation of cybercrime at both national and international levels, as well as the main challenges that arise in combating this type of criminal activity.

Results of the research and their discussion: The development of digital technologies has significantly influenced modern society and created new opportunities for criminal activity. Cybercrime includes illegal actions committed using computers, networks, and the Internet, such as hacking, identity theft, and online fraud. One of the main difficulties in combating cybercrime is its transnational nature, since criminals can operate from different countries. Therefore, effective counteraction to cybercrime requires not only legal regulation but also international cooperation and the improvement of investigative methods.

Cybercrime, like crime, consists of engaging in conduct that has been outlawed by a society because it threatens social order. Cybercrime differs from crime primarily in the way it is committed: real-world criminals use physical tools—such as guns—to commit their crimes; cybercriminals use computer technology to commit cybercrimes. That is, cyberspace becomes the tool criminals use to commit old crimes—like fraud, theft, and extortion—in new ways [1, p. 6].

Nowadays, there are many types of cybercrimes, which affect individuals, organizations, and society as a whole. The most common forms include phishing, identity theft, hacking, ransomware attacks, and cyberbullying. These represent only a part of the wide range of cyber offenses, which also encompass online fraud, spyware, and other malicious activities [2, p. 2-3].

It is believed that the first international initiative relating to the fight against computer crime was taken by the Council of Europe. The initiative in question was the Conference on Criminological Aspects of Economic Crime, held in Strasbourg in 1976, at which an attempt was made to define certain categories of computer-related crimes.

The statement that international cooperation plays an enormous role in the fight against crimes committed on computer networks is undoubtedly a truism. The range of telecommunications networks is vast and worldwide. The conduct of a perpetrator may have simultaneous effects in many countries located at opposite ends of the globe. In addition to close cooperation between law enforcement authorities, it is also important to criminalise computer crime in as many countries as possible until the so-called hackers' paradise, i.e., countries in which their actions remain unpunished, are completely eliminated [3].

At the national level, building on the importance of international cooperation and harmonized cybercrime legislation, the Verkhovna Rada Committee on Digital Transformation, responsible for cybersecurity, deploys a Working Group «On the formation of conditions, creation and management of information cybertechnologies and the formation of national legislation in the field of cybersecurity of Ukraine» at a sufficiently expert and professional level to prepare proposals for improving legislation in regulating
cybersecurity and protection of critical infrastructure.

The Working Group included representatives of national cybersecurity, representatives of cybersecurity from business organizations, cybersecurity experts and representatives of public associations.

The Working Group is currently working on the implementation of the NIS Directive and directives of the United Nations and other international organizations. Information on the draft law on critical infrastructure is more detailed in the section below.

Activity in the direction of improving cybersecurity legislation is related to conclusions of the analysis of cybersecurity legislation contained in numerous expert reports of various institutions and organizations (EU, IFES, MITER and the UNDP) [4, p. 24].

Despite the efforts to strengthen international cooperation and improve legal regulation in the field of cybersecurity, a number of significant challenges remain in combating cybercrime. One of the main difficulties is determining jurisdiction in cybercrime cases due to the borderless nature of the Internet. Cybercriminals may operate from one country while targeting victims in another, making it difficult to determine which country's laws apply and where prosecutions should take place. In the process of prosecuting cybercrime, an important issue is the identification of the true identity and location of cybercriminals. Attackers can use various techniques to hide their tracks, such as routing attacks through multiple servers, using anonymisation tools, and exploiting compromised systems. This makes it difficult to attribute cybercrime to specific individuals or groups. At the same time, extraditing cybercriminals to face justice in another country can be complicated due to legal, political and diplomatic barriers. Some countries may not have appropriate laws to prosecute cybercrime, or they may not consider cybercrime an extraditable offence. In addition, some countries may lack the resources, technology and expertise necessary to effectively investigate and prosecute cybercrime. This may lead to differences in enforcement capabilities across jurisdictions. The speed at which cybercrime occurs and the potential for data loss require a rapid response. However, traditional legal procedures for obtaining evidence can be time-consuming, which may prevent the timely collection of important information. Furthermore, the rapid development of technology often outpaces the development of comprehensive cybercrime laws. Definitions of cybercrime and legal frameworks may differ from country to country, making harmonisation and cooperation more difficult. Ultimately, ensuring the integrity of digital evidence remains crucial in cybercrime prosecutions [5, p. 91].

Conclusion: In summary, cybercrime remains one of the most pressing challenges in modern society, affecting individuals, organizations, and international security. This study has shown that combating cybercrime effectively requires a combination of strong national legislation, harmonized legal frameworks, and active international cooperation. Despite ongoing efforts, challenges such as jurisdictional issues, identification of cybercriminals, differences in enforcement capabilities, and the rapid pace of technological development continue to hinder prosecution and prevention. Ensuring the integrity of digital evidence and continuously improving cybersecurity laws and investigative methods are therefore essential to protect critical infrastructure and maintain public trust in the digital environment.

References:

1. Brenner S. W. *Cybercrime and the Law: Challenges, Issues, and Outcomes* / S. W. Brenner. – Boston : Northeastern University Press, 2010. – 350 p.
2. Tamang S., Chandana G.S., Roy B.K. *Different Cybercrimes and Their Solution for Common People* [Electronic resource] / S. Tamang, G.S. Chandana, B.K. Roy // arXiv. – 2024. – Available at: https://arxiv.org/abs/2410.09089 (accessed: 09.03.2026).
3. Radoniewicz F. *Cybercrime and the Law: An Analysis of Legal Governance in Europe* / F. Radoniewicz. – London : Routledge, 2025. – 280 p.

4. *Ukrainian Cybersecurity Legal Framework: Overview* [Electronic resource]. – IFES Ukraine, 2020-2021. – Available at: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-Legal-Framework-Overview-2020-v2-2021-04-01-Eng.pdf (accessed: 11.03.2026).
5. Macidov S. T. *Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations* / S. T. Macidov // *Futurity Economics & Law*. – 2023. – Vol. 15, No. 3. – P. 45–60.