4. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. Ратифікована Законом України від 17 липня 1997 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 07.05.2026).

5. Тодика О. Ю. Реалізація конституційних норм з прав і свобод людини і громадянина в Україні. Харків: Право, 2011. 256 с.

6. Закон України «Про виконання рішень та застосування практики Європейського суду з прав людини» від 23 лютого 2006 р. № 3477-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 260. URL: https://zakon.rada.gov.ua/laws/show/3477-15 (дата звернення: 05.05.2026).

7. Рабінович П. М. Права людини і громадянина: навч. посіб. Київ: Атіка, 2014. 280 с.

Pyhyda Andrii,
a Master's degree student in Law,
the Educational and Scientific Institute of Law and Psychology, the National Academy of Internal Affairs Scientific Adviser:
Bohutskyi Vadym,
Associate Professor of the Department of Business Ukrainian and Foreign Languages,
the Educational and Scientific Institute of Law and Psychology,
the National Academy of Internal Affairs,
Candidate of Philological Sciences, Associate Professor

INTERNATIONAL LAW ENFORCEMENT COOPERATION IN COMBATING CYBERCRIME: EU EXPERIENCE

Cybercrime represents one of the most dynamic and complex threats of modern times, requiring effective international cooperation among law enforcement agencies. The transnational nature of cybercrimes, their technological complexity, and rapid proliferation make it impossible to combat them at a purely national level. The European Union has developed a comprehensive system of international cooperation that integrates institutional mechanisms, operational platforms, legal instruments, and technological solutions.

The central element of the European system for combating cybercrime is the European Cybercrime Centre (EC3), established within Europol's structure in 2013. EC3 functions as a central platform for coordinating cross-border law enforcement actions against computer crimes and a centre of technical expertise on these issues. Since its inception, EC3 has participated in numerous high-profile operations and hundreds of operational support deployments, resulting in hundreds of arrests. The Centre focuses on three main types of cybercrimes: crimes dependent on cyberspace, online child sexual exploitation, and payment fraud, as well as combating crime in the dark web.

A key operational tool for international cooperation is the Joint Cybercrime Action Taskforce (J-CAT), established in September 2014. J-CAT is the first permanent, physically co-located international operational team for combating cybercrime, consisting of cyber liaison officers from EU member states and partner

countries. As of 2024, J-CAT unites representatives from 16 countries, including nine EU member states (Austria, France, Germany, Italy, the Netherlands, Romania, Poland, Spain, and Sweden) and six partner countries (Australia, Canada, Colombia, Norway, Switzerland, the United Kingdom, and the United States). The flexible bureaucratic structure of J-CAT allows for rapid response to cyber threats and adaptation to changes in the criminal landscape.

The Joint Cybercrime Action Taskforce coordinates international investigations, supporting the exchange of operational information in real-time and the joint conduct of operations against key cyber threats. J-CAT specializes in combating high-tech crimes (malware, botnets, unauthorized intrusions), crime facilitation (bulletproof hosting, anti-antivirus services, infrastructure rental, money laundering, and crimes using virtual currencies), and online fraud. In 2024, thanks to J-CAT's activities, numerous successful operations were conducted, including Operation Endgame, aimed at eliminating botnets and associated criminal infrastructure.

The legal basis for international cooperation in the field of cybercrime is the Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention, adopted in 2001 and entered into force in 2004. This is the first international treaty aimed at harmonizing national laws, improving investigative methods, and strengthening cooperation between countries in combating cybercrime. As of August 2025, 81 states have ratified the Convention. The Budapest Convention defines three key objectives: harmonization of substantive criminal law in the area of cybercrimes, provision of procedural powers for investigating and prosecuting such crimes, and creation of a rapid and effective regime for international cooperation. In 2022, a Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence was developed, which entered into force in 2023. This Protocol addresses the particular problem of electronic evidence stored by service providers in foreign jurisdictions and establishes expanded tools for cross-border cooperation in obtaining electronic evidence, including emergency mutual assistance and video conferencing. The Protocol also creates a network of 24/7 contact points to ensure rapid response in cybercrime investigations.

The European Cybercrime Task Force (EUCTF), established in 2010 jointly by Europol, the European Commission, and EU member states, is a trusted network that brings together heads of national cybercrime units from various member states, as well as representatives from Europol, the European Commission, Eurojust, and the European Police Academy. EUCTF meets twice a year at Europol headquarters to coordinate strategic directions for combating cybercrime.

An important aspect of international cooperation is the joint analysis of challenges in combating cybercrime. In 2024, Eurojust and Europol published a report titled “Common Challenges in Cybercrime”, which highlights both ongoing and emerging challenges in the area of cybercrime and investigations related to digital evidence. The report emphasizes key problems: managing huge volumes of data, loss of access to data, and challenges related to anonymization services. The document also presents new EU legislative frameworks, including the e-evidence Package and the Digital Services Act, designed to address these challenges.

The annual Internet Organised Crime Threat Assessment (IOCTA), published by Europol, is a key analytical tool for identifying priorities in combating cybercrime. The IOCTA 2024 report highlights current trends in cyberattacks, online child sexual

exploitation, and online and payment fraud schemes, noting that recent law enforcement operations have prompted ransomware groups to reorganize their activities.

Thus, international cooperation of EU law enforcement agencies in combating cybercrime is based on an integrated system that combines specialized institutions (EC3, J-CAT, EUCTF), legal frameworks (Budapest Convention and its protocols), operational coordination (EMPACT, joint investigation teams), analytical tools (IOCTA, joint reports from Eurojust and Europol), and technological cooperation with the private sector. The effectiveness of this system is ensured by clear legal regulation, trust relationships among member states, flexible organizational structure, and constant adaptation to changes in the cybercrime environment. The EU experience demonstrates that successful combat against transnational cybercrime is possible only through comprehensive international cooperation that covers all aspects of law enforcement activities.

References:

1. European Cybercrime Centre – EC3. Europol. 2024. URL: European Cybercrime Centre – EC3 (accessed: 07.05.2026).

2. Joint Cybercrime Action Taskforce (J-CAT). Europol. 2024. URL: Joint Cybercrime Action Taskforce (J-CAT) (accessed: 07.05.2026).

3. Common Challenges in Cybercrime: 2024 Review by Eurojust and Europol. Eurojust and Europol. 2024. URL: Common Challenges in Cybercrime: 2024 Review (accessed: 07.05.2026).

4. Convention on Cybercrime (Budapest Convention). Council of Europe. 2001. European Treaty Series No. 185. URL: Convention on Cybercrime (Budapest Convention) (accessed: 07.05.2026).

5. Internet Organised Crime Threat Assessment (IOCTA) 2024. Europol. 2024. URL: Internet Organised Crime Threat Assessment (IOCTA) 2024 (accessed: 07.05.2026).

Стрельцова Кіра Юріївна,
студентка 1 курсу бакалаврату, «Правоохоронна діяльність»
навчально-наукового інституту права та психології
Національна академія внутрішніх справ
Науковий керівник:
Пилипенко Вікторія Вікторівна,
доцент кафедри теорії, історії та філософії права
навчально-наукового інституту права та психології
Національної академії внутрішніх справ,
кандидат історичних наук, доцент

ЦИВІЛЬНІ ПРАВА В УМОВАХ ВІЙНИ: ТРАНСФОРМАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ ТА МЕЖІ ЇХ РЕАЛІЗАЦІЇ В ПЕРІОД ВОЄННОГО СТАНУ В УКРАЇНІ

Збройна російська агресія проти України зумовила трансформацію національної правової системи, актуалізувавши дилему балансу між інтересами національної безпеки та збереженням сутності цивільних прав особи.