**ФІЛІМОНОВ М. В.,**
аспірант кафедри кримінального процесу
*(Національний університет «Одеська юридична академія»)*

**УДК 343.98:004.056:341.01**
**DOI https://doi.org/10.32842/2078-3736/2025.3.2.89**

# МІЖНАРОДНІ СТАНДАРТИ ТА ЗАРУБІЖНИЙ ДОСВІД НОРМАТИВНОЇ РЕГЛАМЕНТАЦІЇ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Стаття присвячена аналізу міжнародних стандартів розслідування кримінальних правопорушень, вчинених у кіберпросторі, в умовах стрімкого розвитку цифрових технологій та зростання їх транскордонного характеру. Обґрунтовано, що поширення кіберзлочинів, вчинених із використанням інформаційно-комунікаційних технологій, зумовлює недостатність суто національних процесуальних механізмів та актуалізує необхідність узгодження правових підходів на міжнародному рівні з метою подолання конфліктів юрисдикцій і забезпечення збирання та використання електронних доказів.

Автор зазначає, що у міжнародно-правовому вимірі провідну роль у формуванні процесуальних стандартів розслідування кіберзлочинів відіграє Конвенція Ради Європи про кіберзлочинність, яка закріплює мінімальні вимоги щодо термінового збереження, обшуку, арешту та перехоплення електронних даних, а також визначає засади міжнародної правової допомоги у кримінальному провадженні.

Наголошено, що право Європейського Союзу демонструє тенденцію до подальшої уніфікації та деталізації процедур доступу до електронних доказів, що відображено у Регламенті (ЄС) 2023/1543, який запроваджує Європейський наказ про надання та збереження електронних доказів і встановлює прямі механізми взаємодії з постачальниками цифрових послуг за умови дотримання принципів необхідності, пропорційності та захисту права на приватність.

Автор підкреслює, що досвід США та Великої Британії ґрунтується на поєднанні суворої криміналізації несанкціонованого доступу до інформаційних систем із розгалуженими процедурами судового контролю за втручанням у сферу електронних комунікацій, що сприяє балансуванню між інтересами ефективного розслідування та гарантіями прав людини.

Автор доходить висновку, що міжнародні стандарти та позитивні зарубіжні практики створюють належне підґрунтя для імплементації в національне законодавство України сучасних процесуальних механізмів доступу до цифрових доказів, розвитку міжнародного співробітництва та посилення судового контролю, необхідних для адаптації кримінального провадження до викликів цифрової епохи.

***Ключові слова:*** *кримінальне провадження, кіберпростір, кіберзлочини, міжнародні стандарти, докази, електронні докази, досудове розслідування, міжнародне співробітництво.*

**Filimonov M. V. International Standards and Foreign Experience of the Regulatory Framework for the Investigation of Criminal Offenses Committed in Cyberspace**

The article is devoted to the analysis of international standards for the investigation of criminal offenses committed in cyberspace in the context of the rapid development of digital technologies and the growing transnational nature of such offenses. It is substantiated that the spread of cybercrimes committed through the use of information and communication technologies reveals the insufficiency of purely national procedural mechanisms and highlights the need to harmonize legal approaches at the international level in order to overcome jurisdictional conflicts and ensure the collection and use of electronic evidence.

The author notes that, in the international legal dimension, a leading role in shaping procedural standards for the investigation of cybercrimes is played by the Council of Europe Convention on Cybercrime, which establishes minimum requirements for the expedited preservation, search, seizure, and interception of electronic data, as well as defines the principles of international mutual legal assistance in criminal proceedings.

It is emphasized that European Union law demonstrates a tendency toward further unification and detailed regulation of procedures for access to electronic evidence, as reflected in Regulation (EU) 2023/1543, which introduces the European Production Order and the European Preservation Order for electronic evidence and establishes direct mechanisms of interaction with digital service providers, subject to compliance with the principles of necessity, proportionality, and the protection of the right to privacy.

The author emphasizes that the experience of the United States and the United Kingdom is based on a combination of strict criminalization of unauthorized access to information systems and extensive procedures of judicial oversight over state interference in the sphere of electronic communications, which contributes to maintaining a balance between the interests of effective investigation and the guarantees of human rights.

The author concludes that international standards and positive foreign practices provide a solid foundation for the implementation into the national legislation of Ukraine of modern procedural mechanisms for access to digital evidence, the development of international cooperation, and the strengthening of judicial control, which are necessary for adapting criminal proceedings to the challenges of the digital age.

***Key words:*** *criminal proceedings, cyberspace, cybercrime, international standards, evidence, electronic evidence, pre-trial investigation, international cooperation.*

**Вступ.** У сучасному світі, у якому цифрові технології стрімко впроваджуються в усі сфери життя суспільства, міжнародні стандарти розслідування кримінальних правопорушень, вчинених у кіберпросторі відіграють ключову роль у забезпеченні ефективної протидії цим правопорушенням.

У кримінальній процесуальній, криміналістичній та кримінологічній доктрині практично беззаперечною є така іманентна ознака кіберзлочинів як транскордонний характер, коли сервери, потерпілий, а також особи, які підозрюються або обвинувачуються у їх вчиненні можуть перебувати у різних країнах, що робить суто національні правові механізми притягнення до відповідальності недостатніми. У цьому контексті, узгодження правової політики щодо розслідування відповідної категорії кримінальних правопорушень на основі міжнародних стандартів у цій сфері є необхідною передумовою подолання потенційних

конфліктів юрисдикцій та вироблення спільних підходів до здіснення кримінального переслідування.

Переважна більшість міжнародних стандартів у досліджуваній царині присвячена уніфікації кримінально-правових підходів у релевантних питаннях. Зокрема, міжнародні акти закріплюють поняття кіберзлочинів, визначають мінімальні вимоги до їх криміналізації та окремі підходи до кваліфікації відповідних діянь. Втім, кримінальні процесуальні аспекти розслідування кримінальних правопорушень у кіберпросторі також мають під собою вагоме нормативне підгрунтя, адже транскордонних характер відповідних правопорушень обумовлює необхідність задіяння механізмів міжнародної правової допомоги, обміну інформацією та доступу до тих даних, що перебувають у закордонних провайдерів.

Питання розслідування кримінальних правопорушень, вчинених у кіберпросторі у доктрині досліджувались І.І. Васильковським, О.Ю. Довженко, П.П. Галушко, І.Г. Каланчею, Я.В. Неділько, Д.В. Пашнєвим, О.А. Самойленко, В.В. Сисолятіним, В.А. Сусукайлом, А.В. Ратновою, А.В. Рейнгольдом, Б.Б. Теплицьким, Д.М. Цеханом, М.Ю. Яцишин. Утім, проблемам міжнародних стандартів у цій царині та зарубіжного досвіду присвячені лише окремі праці. Винятком є лише дисертаційне дослідження М.Ю. Яцишин «Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю» (м. Київ, 2019), однак воно присвячено здебільшого питанням міжнародного співробітництва у сфері протидії кіберзлочинності, а не проблемам розслідування правопорушень, вчинених у кіберпросторі.

**Постановка проблеми.** Мета статті полягає у визначенні міжнародних стандартів розслідування кримінальних правопорушень, вчинених у кіберпросторі, виявленні позитивних зарубіжних практик нормативної регламентації розслідування кримінальних праворушень, вчинених у кіберпросторі та встановлення можливості їх імплементації у вітчизняне законодавство.

**Результати досліджень**. За останні два десятиліття було прийнято низку міжнародно-правових актів, спрямованих на співробітництво держав у сфері боротьби із кіберзлочинністю. М.Ю. Яцишин зазначає, що сучасній стадії розвитку інституту міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю притаманний регіональний характер та інтенсифікація уніфікації національних законодавств [1, с. 41]. Такий висновок авторка робить, зокрема, й через відсутність універсальних міжнародних актів у цій сфері.

В межах Ради Європи основним документом, який визначає засади співробітництва держав у галузі боротьби із кіберзлочинністю є Конвенція про кіберзлочинність Ради Європи, прийнята 21.11.2001 р. (Будапештська Конвенція) та Додатковий протокол до неї від 28.01.2003 р.

Друга частина розділу 2 Будапештської конвенції має назву «Процедурне право» і вона містить мінімальні стандарти щодо законодавчих та інших заходів, які можуть бути необхідними для здійснення конкретних кримінальних розслідувань або переслідувань. У п. «с» п. 2 ст. 14 Конвенції зазначено, що відповідні правила і процедури поширюються на збір доказів у електронній формі стосовно кримінального правопорушення [2].

Серед заходів, які можуть бути вжиті Сторонами, спрямовані на співробітництво у питаннях розслідування кримінальних правопорушень, вчинених у кіберпросторі Конвенцією визначені: 1) термінове збереження комп'ютерних даних, які зберігаються (ст. 16); 2) термінове збереження і часткове розкриття даних про рух інформації (ст. 17); 3) обшук і арешт комп'ютерних даних, які зберігаються (ст. 19); 4) збирання даних про рух інформації у реальному масштабі часу (ст. 20); 5) перехоплення даних змісту інформації (ст. 21). Крім того, Будапештська конвенція визначає засади міжнародного співробітництва держав, у тому числі взаємної правової допомоги при розслідуванні кіберзлочинів.

На рівні права ЄС питання міжнародного співробітництва у сфері розслідування кримінальних правопорушень, вчинених у кіберпросторі регламентуються двома основними актами: 1) Директива (ЄС) 2022/2555 Європейського парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в усьому Союзі, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви

(ЄС) 2016/1148 (Директива NIS 2) (далі – Директива (ЄС) 2022/2555) [3]; 2) Регламент (ЄС) 2023/1543 Європейського парламенту та Ради від 12 липня 2023 року «Про Європейські процедурні накази та Європейські накази про збереження електронних доказів у кримінальному провадженні та для виконання вироків позбавлення волі після кримінального провадження» (далі – Регламент ЄС) 2023/1543) [4].

Директива (ЄС) 2022/2555) містить Розділ 6, який має назву «Обмін інформацією». Ст. 29 Директиви передбачає, що Держави-члени забезпечують, щоб суб'єкти, які підпадають під дію цієї Директиви, та, де це доречно, інші суб'єкти, які не підпадають під дію цієї Директиви, могли добровільно обмінюватися між собою відповідною інформацією про кібербезпеку, включаючи інформацію, що стосується кіберзагроз, недоліків, вразливості, методи та процедури, інформацію про суб'єкта загрози, попередження про кібербезпеку та рекомендації щодо конфігурації інструментів кібербезпеки для виявлення кібератак, де такий обмін інформацією: а) має на меті запобігти, виявити, реагувати або відновитися після інцидентів або пом'якшити їх вплив; б) підвищує рівень кібербезпеки, зокрема, шляхом підвищення обізнаності щодо кіберзагроз, обмеження або перешкоджання здатності таких загроз поширюватися, підтримує низку оборонних можливостей, усуває та розкриває вразливості, методи виявлення, стримування та запобігання загрозам, стратегії пом'якшення наслідків або етапи реагування та відновлення або сприяє спільним дослідженням кіберзагроз між державними та приватними суб'єктами [3].

До сфери кримінального провадження більш дотичним є Регламент ЄС) 2023/1543. У п. 23 Регламенту визначено, що «оскільки провадження щодо взаємної правової допомоги може розглядатися як кримінальне провадження відповідно до чинного національного законодавства в державах-членах, слід уточнити, що Європейський наказ про надання електронних доказів або Європейський наказ про збереження не повинні видаватися для надання взаємної правової допомоги іншій державі-члену або третій країні. У таких випадках запит на взаємну правову допомогу повинен бути спрямований до держави-члена або третьої країни, яка може надати взаємну правову допомогу відповідно до свого національного законодавства». При цьому, у межах кримінального провадження Європейський наказ про надання електронних доказів та Європейський наказ про збереження повинні бути видані лише для конкретного кримінального провадження щодо конкретного кримінального правопорушення, яке вже відбулося, після індивідуальної оцінки необхідності та пропорційності цих наказів у кожній окремій справі, з урахуванням прав підозрюваного або обвинуваченої особи (п. 24 Регламенту) [4].

У Регламенті достатньо серйозна увага приділяється стандартам щодо забезпечення права на приватність при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі. У п. 33 визначено, що у випадку якщо IP-адреси, номери доступу та пов'язана з ними інформація не запитуються з єдиною метою ідентифікації користувача в конкретному кримінальному розслідуванні, то, як правило, має запитуватися більш деталізована інформація, що стосується конфіденційності, така як контакти та місцезнаходження користувача. Таким чином, вони можуть служити для встановлення комплексного профілю особи, але в той же час їх можна обробляти та аналізувати легше, ніж дані про вміст, оскільки вони представлені в структурованому та стандартизованому форматі. Тому важливо, щоб у таких ситуаціях IP-адреси, номери доступу та пов'язана з ними інформація, які не запитуються з єдиною метою ідентифікації користувача в конкретному кримінальному розслідуванні, розглядалися як дані про трафік і запитувалися в тому ж режимі, що і дані про зміст[4].

Регламент регулює й випадки, коли захищені дані підпадають під дію імунітетів та привілеїв відповідно до законодавства окремих Держав-членів. У п.48 встановлено, що якщо орган, який видав документ, прагне отримати дані про трафік і має обґрунтовані підстави вважати, що запитувані дані захищені імунітетами або привілеями, наданими відповідно до законодавства держави-виконавця, або що ці дані підпадають під дію в цій державі правил визначення та обмеження кримінальної відповідальності, що стосуються свободи преси та свободи вираження поглядів в інших засобах масової інформації, орган, що видав,

повинен мати можливість шукати роз'яснення перед видачею Європейського наказу про надання електронних доказів, в тому числі шляхом консультацій з компетентними органами держави-виконавця або безпосередньо, або через Євроюст та Європейську судову мережу.

У контексті актів права ЄС, які регламентують питання розслідування кримінальних правопорушень, учинених у кіберпросторі окрему увагу слід приділити також й Резолюції Європейського Парламенту від 3 жовтня 2017 року про боротьбу з кіберзлочинністю (2017/2068(INI)) (2018/C 346/04). У ній підкреслено необхідність розробки спільних процедурних стандартів, які враховуватимуть територіальні фактори та визначатимуть слідчі заходи, які можуть використовуватися незалежно від географічних кордонів [5].

У США чинними є низка законодавчих актів, які встановлюють федеральні правила та процедуру доступу до електронних доказів. Одним із ключових законів у цій галузі є закон 18 U.S.C. § 1030- Computer Fraud and Abuse Act (CFAA) [6], який встановлює кримінальну та цивільну відповідальність за несанкціонований доступ до комп'ютерів і пов'язані з цим зловживання. Він містить перелік окремих діянь, які є кримінальними правопорушеннями, пов'язаними із незаконним доступом до інформаційних систем, серед яких отримання інформації незаконним шляхом, комп'ютерне шахрайство, заподіяння шкоди комп'ютерним системам, торгівля засобами доступу (паролі, коди), вимагання, пов'язане з комп'ютерною шкодою тощо. Закон встановлює правило екстериторіальності, якt передбачає, що закон є застосовним, у тому числі, у випадках, коли шкода заподіяна комп'ютеру в США, незалежно від місця перебування злочинця.

Іншим федеральним законом США, який оновив правове регулювання приватності комунікацій у цифрову епоху є Electronic Communications Privacy Act (ECPA) of 1986 [7]. Закон містить загальне правило судового контролю доступу до комунікацій, а також встановлює різні типи режимів доступу правоохоронних органів до абонентських даних.

Низка спеціалізованих законів щодо процедур розслідування кримінальних правопорушень, вчинених у кіберпросторі є й у Великій Британії. Ключовим у цьому контексті є Computer Misuse Act 1990 [8]. Відповідним законом криміналізовано низку діянь, зокрема, несанкціонований доступ до комп'ютерних систем та даних, несанкціоновані дії зі знищення, пошкодження або перешкоджання роботі комп'ютерів, а також отримання або створення інструментів для здійснення таких злочинів. У контексті розслідування злочинів у цифровому середовищі, основним законодавчим актом є Investigatory Powers Act 2016 (IPA) [9]. Закон створює правову основу для доступу до даних пристроїв під час розслідувань та встановлює судовий контроль за видачею дозволів на проникнення в цифрові системи.

Окремі питання доступу правоохоронних органів до цифрових даних викладені також і у Data Protection Act 2018 (DPA 2018) [10]. У законі встановлено спеціальні правила обробки компетентними органами цифрової інформації, зокрема, має чітко визначатись мета обробки, дані повинні бути релевантними розслідуванню та не надмірними (п.37).

**Висновок.** Отже, аналіз міжнародних стандартів та зарубіжного законодавства у сфері розслідування кримінальних правопорушень, вчинених у кіберпросторі, свідчить про поступове формування багаторівневої системи правового регулювання, спрямованої на забезпечення ефективної протидії кіберзлочинності в умовах її транскордонного характеру. Ключовим орієнтиром у цій сфері залишаються міжнародні стандарти, які забезпечують узгодження національних правових підходів, мінімізацію конфліктів юрисдикцій та створення спільних механізмів збору й використання електронних доказів.

Будапештська конвенція Ради Європи закріплює фундаментальні процесуальні інструменти розслідування кіберзлочинів і формує базові принципи міжнародного співробітництва. Водночас, право Європейського Союзу демонструє тенденцію до подальшої деталізації та уніфікації процедур доступу до електронних доказів, що яскраво проявляється у Регламенті (ЄС) 2023/1543, який запроваджує прямі механізми взаємодії з постачальниками цифрових послуг за умови дотримання принципів необхідності, пропорційності та захисту права на приватність.

Досвід США та Великої Британії засвідчує поєднання суворої криміналізації несанкціонованого доступу до інформаційних систем із розгалуженими процедурами судового контролю за втручанням держави у сферу електронних комунікацій. Особливу увагу у цих правопорядках приділено балансуванню між інтересами ефективного розслідування та гарантіями прав людини, насамперед права на повагу до приватного життя та захист персональних даних.

Загалом, міжнародні стандарти та позитивні зарубіжні практики свідчать про необхідність подальшої імплементації у національне законодавство України сучасних процесуальних механізмів доступу до цифрових доказів, розвитку міжнародного співробітництва та забезпечення належного рівня судового контролю. Це є важливою передумовою адаптації кримінального провадження до викликів цифрової епохи та підвищення ефективності розслідування кримінальних правопорушень, вчинених у кіберпросторі.

**Список використаних джерел:**

1. Яцишин М.Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю: дис. …канд. юрид. наук. 12.00.11. Київ, 2019. 230 с.

2. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

4. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng

5. European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2018_346_R_0005&utm_

6. Computer Fraud and Abuse Act (CFAA). URL: https://www.justice.gov/jm/jm-9-48000-computer-fraud

7. Electronic Communications Privacy Act of 1986. URL: https://www.congress.gov/bill/99th-congress/house-bill/4952

8. Computer Misuse Act 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents

9. Investigatory Powers Act 2016. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents

10. Data Protection Act 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents