

Кіберзлочинність та діяльність Інтерполу щодо розкриття злочинів у сфері високих технологій

Тетяна Кривак,

Київський НДІСЕ, м. Київ, Україна, ORCID: <https://orcid.org/0000-0002-0679-1080>,
e-mail: t.kryvak@kndise.gov.ua

Розглянуто особливості кіберзлочинності як суспільно-небезпечного явища та його вплив на міжнародну безпеку. Акцентовано увагу на діяльність Інтерполу щодо координації співробітництва держав у боротьбі з кіберзлочинністю та проаналізовано основні резолюції щодо злочинів у сфері високих технологій, що були прийняті Інтерполом.

Ключові слова: кіберзлочинність; кіберпростір; резолюція; Інтерпол.

Cybercrime and Interpol's activities regarding the disclosure of crimes in the field of high technologies

Tetiana Kryvak

The features of cybercrime as a socially dangerous phenomenon and its impact on international security are considered. Attention is focused on the activities of Interpol in coordinating cooperation between states in the fight against cybercrime and the main resolutions on crimes in the field of high technologies adopted by Interpol are analyzed.

Keywords: cybercrime, cyberspace, resolution, Interpol.

Природа кіберзлочинності та породжувані нею правові проблеми транснаціональні. Поняття «кіберзлочинність» уперше з'явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів відносно автоматизованих систем обробки даних. Поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, у якому відбуваються правопорушення, і засобом або знаряддям злочину. Отже, кіберзлочинність може бути визначена як сукупність злочинів, скоєних у кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, проти комп'ютерних систем, мереж і даних [1]. Актуальність даної теми зумовлена тим, що транснаціональний характер злочинності у сфері високих технологій потребує узгоджених міжнародних зусиль боротьби з нею.

Зважаючи на той факт, що з кожним днем кіберзлочинність зростає та розповсюджується, і жодна держава сьогодні вже не спроможна самостійно протистояти цій небезпеці, з'явилася необхідність активізації міжнародного співробітництва в цій сфері. Інтерпол був першою міжнародною організацією, яка спробувала

співвіднести комп'ютерні злочини та кримінальне законодавство, оскільки саме Інтерпол координує співробітництво держав у боротьбі зі злочинністю у сфері високих технологій.

Варто зазначити, що особливу значущість дана проблема отримала у зв'язку із пандемією та переходом громадян на дистанційну форму роботи. Це, своєю чергою, призвело до росту інтернет-злочинів і підтверджується звітом Інтерполу, опублікованим на офіційному сайті організації. Відповідно до зазначеного звіту, кіберзлочинці, які раніше зосереджували свою увагу на дрібних підприємцях, під час пандемії коронавірусу спрямували свої хакерські атаки на великі корпорації та уряди [2].

Діяльність Інтерполу щодо координації співробітництва держав у боротьбі з кіберзлочинністю здійснюється його органами. В Інтерполі центральними органами управління є Генеральна Асамблея, найвищий пленарний орган Інтерполу, та Виконавчий комітет — найвищий адміністративно-виконавчий орган [3]. Відповідно до ст. 25 Статуту постійною службою Інтерполу є Генеральний секретаріат. Відповідно до ст. 26 Статуту Генеральний секретаріат утілює в життя рішення Генеральної Асамблеї та Виконавчого комітету; виступає як міжнародний центр боротьби зі злочинністю; діє як спеціалізований та інформаційний центр; здійснює ефективне керівництво діяльністю організації; підтримує контакти з національними та міжнародними

органами (причому питання, пов'язані з розшуком злочинців, розв'язуються через національні центральні бюро) та ін. [4].

Згідно з Конвенцією Ради Європи з боротьби із кіберзлочинністю, яка була ратифікована і Верховною Радою України, виділено чотири основних типи кіберзлочинів [5], а саме:

- 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему, зловживання пристроями);
- 2) правопорушення, пов'язані з комп'ютерами (підробка, шахрайство);
- 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);
- 4) правопорушення, пов'язані з порушенням авторських або суміжних прав.

Відповідно до цього Генеральною Асамблеєю Інтерполу було прийнято ряд документів щодо злочинів у сфері високих технологій, а саме:

- Резолюції щодо створення структурних підрозділів Інтерполу із боротьби зі злочинністю у сфері високих технологій. 2008 р. було схвалено Резолюцію № AG-2008-RES-08 «Створення підрозділу з проведення судової комп'ютерної експертизи» [6] із метою забезпечення відповідного навчання держав-членів, особливо фахівців у галузі оперативно-розшукової діяльності; організації та координації, на запит держав-членів надання допомоги у проведенні неупередженої та незалежної комп'ютерної судової експертизи із залученням відповідних експертів; створення міжнародних стандартів у сфері пошуку, виїмки та дослідження електронних доказів.
- Резолюції щодо протидії міжнародній торгівлі дитячою порнографією через Інтернет. Зокрема, Резолюція № AGN/65/RES/9 «Міжнародна торгівля дитячою порнографією» [7]. Згідно з цим документом державам-членам слід ввести кримінальну відповідальність за виробництво, розповсюдження, ввезення або володіння дитячою порнографією, а також підбурювання до вчинення даного діяння та допомогу, передбачити законодавчі норми, які дозволяють конфісковувати майно, отримане завдяки цим злочинам. У документі звернено увагу на те, що в законодавстві треба

враховувати спосіб скоєння злочинів. Резолюція закликає країни-учасниці надати максимальної важливості розслідуванню випадків поширення дитячої порнографії за допомогою інформаційно-комунікаційних технологій, а також передбачити заходи щодо захисту інтересів дитини під час розслідування такої справи. Резолюція № AG-2005-RES-09 «До питання про вебсайти, які продають дитячу порнографію та торгують дітьми» заохочує введення державами-членами відповідних норм до кримінально-процесуального законодавства, що закріплюють процедури співпраці правоохоронних органів з метою сприяння міжнародним розслідуванням стосовно вебсайтів, які продають дитячу порнографію. Відповідно до цієї резолюції національні центральні бюро держав-учасниць мають збільшити обмін інформацією про міжнародні злочинні мережі та злочинців, зайнятих будь-якими формами торгівлі дітьми та виробництвом матеріалів дитячої порнографії, а також повідомляти про всіх ідентифікованих дітей та злочинців Генеральному Секретаріату, щоб уникнути дублювання роботи [8].

- Резолюції щодо протидії діяльності із заохочення тероризму в Інтернеті. До актів такого виду належить Резолюція № AG-2005-RES-10 «До питання про діяльність, що ведеться в інтернеті щодо заохочення тероризму», яка закликає держави-учасниці прийняти законодавство та встановити ефективні процесуальні норми, які уповноважують розпочати міжнародне розслідування та судове переслідування стосовно вебсайтів, які підтримують терористів [9].
- Резолюції щодо протидії злочинам, пов'язаним із наркотиками та Інтернетом. Генеральною Асамблеєю Інтерполу було прийнято Резолюцію № AG-2006-RES-12 «Злочини, пов'язані з наркотиками та Інтернетом», яка рекомендує державам інтенсифікувати співпрацю з цієї проблеми [10].

У своїй структурі Інтерполом були створені підрозділи, які спеціалізуються на боротьбі з кіберзлочинами. На сьогодні в Інтерполі функціонує *Cyber Fusion Center (CFC)*, який об'єднує кіберекспертів із правоохоронних органів і промисловості для збору й аналізу всієї доступної

інформації про злочинну діяльність у кіберпросторі, щоб надавати країнам узгоджені, дієві розвідувальні дані. *CFC* публікує звіти, щоб попередити країни про нові, неминучі або нові кіберзагрози. Із 2017 року було складено понад 800 звітів та направлено поліції у більше ніж 150 країн [11].

Інтерпол також проводить спеціальні операції, направлені на боротьбу з кіберзлочинами. Наприклад, під час десятиденної операції *Falcon II* з 13—22 грудня 2022 року поліція Нігерії заарештувала 11 підозрюваних учасників кіберзлочинної мережі в межах операції національної поліції, координованої з Інтерполом. Підозрювані вважаються членами «*SilverTerrier*», мережі, пов'язаної із шахрайством *Business Email Compromise (BEC)*, яка завдала шкоди тисячам компаній у всьому світі [12].

Отже, можна зробити висновок, що в умовах постійного вдосконалення методів та засобів скоєння кіберзлочинів зростає значення діяльності Інтерполу як універсальної міжнародної організації, яка здійснює координацію співробітництва держав у боротьбі зі злочинністю у сфері високих технологій.

Перелік джерел посилання

1. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки*. 2009. Вип. 19. С. 338—342.
2. Interpol report shows alarming rate of cyberattacks during COVID-19. URL: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19> (дата звернення: 10.03.2023).
3. Governance of Interpol. URL: <https://www.interpol.int/en/Who-we-are/Governance> (дата звернення: 10.03.2023).
4. Interpol's Legal Documents. URL: <https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents> (дата звернення: 10.03.2023).
5. Кіберзлочинність в Україні. Ера цифрових технологій — ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 10.03.2023).
6. Creating an INTERPOL Computer Forensic Analysis Unit. URL: <https://www.interpol.int/content/download/6016/file/AG-2008-77-RES-08%20%20Creating%20an%20INTERPOL%20Computer%20Forensic%20Analysis%20Unit%20.pdf> (дата звернення: 10.03.2023).
7. Resolution No. AGN/65/RES/9. International traffic in child pornography URL: <https://www.interpol.int/Search-Page?&type=document&category=0&year=0&limit=12&search=Resolution%20No.%20AGN/65/RES/9> (дата звернення: 10.03.2023).
8. Resolution No. AG-2005-RES-09. Addressing WebSites selling Child Pornography and Trafficking of Children on Internet. URL: <https://www.interpol.int/Search-Page?&type=document&category=0&year=0&limit=12&search=GA-2005-74-RES-09> (дата звернення: 10.03.2023).
9. Resolution No. AG-2005-RES-10. Addressing Internet activities supporting terrorism. URL: <https://www.interpol.int/Search-Page?&type=document&category=0&year=0&limit=12&search=GA-2005-74-RES-10> (дата звернення: 10.03.2023).
10. Resolution No. AG-2006-RES-12. Internet related drug offences. URL: <https://www.interpol.int/Search-Page?&type=document&category=0&year=0&limit=12&search=AG-2006-RES-12> (дата звернення: 10.03.2023).
11. Cybercrime threat response. URL: <https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response> (дата звернення: 10.03.2023).
12. Nigerian cybercrime fraud: 11 suspects arrested; syndicate busted. URL: <https://www.interpol.int/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted> (дата звернення: 10.03.2023).