

ШАХРАЙСТВО З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ЯК ФОРМА ТРАНСНАЦІОНАЛЬНОЇ КІБЕРЗЛОЧИННОСТІ

Катерина ВІРСЬКА

*аспірантка кафедри кримінального права
Національний юридичний університет імені Ярослава Мудрого
м. Харків, Україна*

Шахрайство з використанням електронно-обчислювальної техніки (далі – ЕОТ) відноситься до кіберзлочинності і на сьогодні має окремі ознаки транснаціональних злочинів, що випливає з положень ч. 2 ст. 3 Конвенції ООН проти транснаціональної організованої злочинності, якщо злочин пов'язаний з кількома державами (за місцем вчинення, підготовки або наслідків)¹. Для ефективної протидії цьому явищу в майбутньому бажано визнати шахрайство з використанням ЕОТ кіберзлочином і віднести його до транснаціонального злочину на міжнародному та національному рівні.

Шахрайство з використанням ЕОТ є динамічно еволюційним і суспільно небезпечним явищем, що характеризується високим рівнем організованості та технологічності. Його транснаціональний характер проявляється у вчиненні злочинів із використанням інфраструктури, розміщеної в різних юрисдикціях, а також у спрямуванні протиправних дій проти осіб чи організацій, що перебувають за межами держави проживання правопорушників. Це зумовлює необхідність міжнародного співробітництва та гармонізації законодавства. Водночас ефективна протидія таким правопорушенням ускладнюється високою латентністю через складність виявлення та небажання потерпілих повідомляти про злочини².

Шахрайство з використанням ЕОТ можна виокремити як одну з найбільш поширених і швидко зростаючих форм транснаціональної злочинності, що має значні економічні та соціальні наслідки. За даними Інтерполу 2024 р., кількість випадків пов'язаних із шахрайством суттєво зросла, а збитки сягають понад 1 млрд доларів, що підтверджує його

¹ Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : від 15.11.2000. Дата оновлення: 04.02.2004. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення: 19.03.2026).

² Коба В. В. Особливості правового регулювання кіберзлочинності в Україні // *Modern scientific journal (Сучасний науковий журнал)*. 2024. № 3(1). С. 32–37. DOI: <https://doi.org/10.36994/2786-9008-2024-3-4>

масштаб і транснаціональний характер. Відповідно до оцінки загроз Інтерполу за 2026 р., фінансове шахрайство стало ключовим елементом полкримінальної діяльності, пов'язаною з організованою злочинністю, кіберзлочинністю та торгівлею людьми. Розвиток штучного інтелекту та доступних цифрових інструментів підвищив ефективність і прибутковість злочинних схем, що разом із поширенням так званих «центрів шахрайства» у різних регіонах світу³ свідчить про глобалізацію цієї загрози.

У щорічному звіті Департаменту кіберполіції за 2025 р. шахрайство з використанням ЕОТ можна виділити як одну з ключових форм транснаціональної кіберзлочинності. Організовані групи (зокрема у складі 20 осіб) через фішингові посилання в соцмережах, месенджерах, Telegram-ботах та підроблені сайти заволодівали коштами громадян України, Польщі, Чеської Республіки та інших країн ЄС, яким спричинено матеріальних збитків на суму понад 1,5 млн грн. Ефективною відповіддю на ці виклики стали міжнародні операції (зокрема «Vicarius») та запуск системи «Antifraud». Завдяки останній, з травня 2025 р. вдалося виявити понад 4,5 тис. інцидентів онлайн-шахрайств із платіжними реквізитами та заблокувати 145 млн грн, які належали потерпілим⁴. Це підтверджує, що шахрайство з використанням ЕОТ є організованим, транснаціональним і потребує міжнародної співпраці для ефектвної протидії.

Сутність транснаціональних кіберзлочинів полягає у вчиненні суспільно небезпечних протиправних діянь у межах інформаційного простору, що функціонує на основі мережі Інтернет, телекомунікаційних мереж, комп'ютерних систем та інших пристроїв обробки інформації. Таке середовище забезпечує обмін даними на основі уніфікованих стандартів і протоколів, що значно розширює можливості для вчинення злочинів⁵.

Ключовим міжнародним актом у сфері протидії кіберзлочинності є Конвенція Ради Європи про кіберзлочинність 2001 р. (Будапештська конвенція), ратифікована Україною у 2005 р., яка безпосередньо передбачає у ст. 8 шахрайство, пов'язане з комп'ютерами. Крім того, дана Конвенція закріплює механізми міжнародного співробітництва, зокрема

³ INTERPOL report warns of increasingly sophisticated global financial fraud threat. *INTERPOL News*. 2026. 16 March. URL: <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat> (дата звернення: 19.03.2026).

⁴ Департамент кіберполіції Національної поліції України. Щорічний звіт за 2025 рік : офіц. звіт. Київ, 2026. 31 с. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/> (дата звернення: 19.03.2026).

⁵ Самойленко О. А., Цехан Д. М. Транснаціональні кіберзлочини : навч.-метод. посіб. для здобувачів вищої освіти / О. А. Самойленко, Д. М. Цехан ; Нац. ун-т «Одес. юрид. академія». Одеса : Фенікс, 2024. 136 с.

екстрадицію, взаємну правову допомогу та процедури збереження електронних доказів⁶. Подальший розвиток міжнародних стандартів відбувся із прийняттям Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів 2022 р., який спрямований на посилення механізмів доступу до електронних доказів і забезпечення ефективного транскордонного співробітництва, зокрема шляхом удосконалення взаємодії між державами та приватним сектором⁷.

Важливу роль у формуванні правових підходів до протидії кіберзлочинності відіграють нормативні акти Європейського Союзу. Зокрема, Директива (ЄС) 2019/713 встановлює мінімальні правила криміналізації шахрайства із використанням безготівкових платіжних засобів, включаючи електронні платіжні інструменти та цифрові валюти⁸. Водночас Директива 2013/40/ЄС передбачає криміналізацію незаконного доступу до інформаційних систем, втручання в їх функціонування та використання спеціальних засобів для вчинення кіберзлочинів⁹. Дані Директиви сприяють уніфікації підходів до захисту цифрового простору та підвищенню ефективності боротьби з кіберзагрозами, зокрема шахрайством з використанням ЕОТ.

Порівняльний аналіз кримінального законодавства окремих європейських держав свідчить про наявність диференційованих підходів до криміналізації діянь, пов'язаних із протиправним використанням ЕОТ з метою отримання майнової вигоди. Зокрема, у Німеччині та Польщі передбачено спеціалізовані норми, що безпосередньо встановлюють відповідальність за комп'ютерне шахрайство як різновид посягання на майнові відносини, що здійснюється шляхом незаконного впливу на процеси обробки даних, використання недостовірної інформації або несанкціонованого втручання в інформаційні системи.

⁶ Конвенція про кіберзлочинність від 23 листоп. 2001 р. (ратифікована Законом України від 07 верес. 2005 р. № 2824-IV). URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 17.03.2026).

⁷ Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224> (дата звернення: 19.03.2026).

⁸ Директива (ЄС) 2019/713 Європейського парламенту і Ради від 17 квіт. 2019 р. про боротьбу з шахрайством і підбрюхою безготівкових платіжних засобів та заміну Рамкового рішення Ради 2001/413/JHA. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0713> (дата звернення: 18.03.2026).

⁹ Директива 2013/40/ЄС Європейського парламенту і Ради від 12 серп. 2013 р. про атаки проти інформаційних систем та заміну Рамкового рішення Ради 2005/222/JHA. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040> (дата звернення: 18.03.2026).

Максимальна санкція за вчинення такого злочину становить до п'яти років позбавлення волі^{10 11}.

У Франції відповідні діяння не розглядаються як шахрайство у класичному розумінні. Зокрема, відповідно до ст. 323-3 Кримінального кодексу Франції, кримінально караними визнаються неправомірне внесення даних до автоматизованої системи обробки інформації, а також їх зміна, видалення, вилучення, відтворення чи передача. Такі дії охоплюються нормами про злочини проти автоматизованих систем обробки даних і тягнуть за собою покарання у вигляді позбавлення волі строком до п'яти років та штраф у розмірі 150 000 євро¹².

Отже, європейські держави застосовують різні підходи до криміналізації комп'ютерно-орієнтованих посягань на майнові відносини: Німеччина та Польща прямо кваліфікують їх як комп'ютерне шахрайство, тоді як Франція відносить їх до атак на автоматизовані системи обробки даних. Водночас, попри відмінності в юридичній кваліфікації, рівень кримінальної відповідальності є подібним і передбачає суворі санкції.

В Україні кримінальна відповідальність за шахрайство з використанням ЕОТ передбачена ч. 4 ст. 190 Кримінального кодексу України (далі – КК України), яка є спеціальною нормою і встановлює покарання у вигляді позбавлення волі на строк від трьох до восьми років¹³. У проєкті нового КК України відбувається відмова від застарілого терміна «електронно-обчислювальна техніка» на користь ширшого поняття «інформаційні системи», що охоплює автоматизовані, електронні комунікаційні та інформаційно-комунікаційні технології. У проєкті передбачено криміналізацію несанкціонованого доступу до інформаційної системи або її частини, незаконне перехоплення комп'ютерних даних (під час їх виходу з інформаційної системи, надходження до неї або при операції з ними всередині інформаційної системи), а також незаконного поводження з комп'ютерними даними,

¹⁰ Article 287 // Penal Code. Chapter XXXV. Poland / United Nations Office on Drugs and Crime (UNODC). SHERLOC. URL: https://www.unodc.org/cld/ru/legislation/pol/penal_code/chapter_xxxv/article_287/article_287.html (дата звернення: 17.03.2026).

¹¹ *German Criminal Code (Strafgesetzbuch – StGB)* : Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 (2) of the Act of 7 November 2024 (Federal Law Gazette 2024 I No. 351) / translation provided by Prof. Dr. Michael Bohlander ; translation revised and updated by Ute Reusch. URL: https://www.gesetz-im-internet.de/englisch_stgb/englisch_stgb.html (дата звернення: 17.03.2026).

¹² Code pénal : version en vigueur au 19 mars 2026 : Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8) // Légifrance : le service public de la diffusion du droit. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149839/ (дата звернення: 17.03.2026).

¹³ *Кримінальний кодекс України* : Закон України від 05 квіт. 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 16.03.2026).

що охоплює їх знищення, пошкодження, блокування, порушення цілісності, порядку маршрутизації чи спотворення процесу обробки. Відповідні правопорушення передбачають санкції у вигляді штрафу або обмеження свободи чи ув'язнення на строк до 2 років¹⁴. Такий перехід від спеціалізованої норми ч. 4 ст. 190 КК України до загальніших норм про інформаційні системи відображає сучасну тенденцію, але водночас вимагає збереження кваліфікації шахрайства з ЕОТ як самостійного майнового транснаціонального злочину.

Отже, шахрайство з використанням ЕОТ доцільно розглядати не лише як злочин проти власності, а як самостійну форму транснаціональної кіберзлочинності. Його специфіка зумовлена поєднанням технологічного середовища вчинення, транснаціонального характеру та високого рівня організованості. Ефективна протидія таким правопорушенням можлива лише за умови комплексного підходу, що включає гармонізацію кримінального законодавства з міжнародно-правовими актами, розвиток міжнародного співробітництва та удосконалення механізмів роботи з електронними доказами. На нашу думку, доцільним є закріплення у новому КК України складу окремого кримінального правопорушення «комп'ютерного шахрайства» за зразком норм Конвенції Ради Європи про кіберзлочинність 2001 р. та законодавства країн ЄС, замість його включення до загальних норм, що регулюють посягання на інформаційні системи.

¹⁴ *Проект Кримінального кодексу України* (станом на 22 лютого 2026 р.). URL: <https://newcriminalcode.org.ua/criminal-code> (дата звернення: 19.03.2026).