

Петро Петрович ГАЛУШКО*(Харківський національний університет внутрішніх справ, м. Харків)*

КІБЕРЗЛОЧИННІСТЬ У ФОКУСІ КРИМІНОЛОГО-ФЕНОМЕНОЛОГІЧНОГО АНАЛІЗУ

Кіберзлочинність зачіпає всі верстви населення як в нашій державі, так і у світі. Найгостріше проблема проявляє себе у площині поширення шайхрайств, порушень сфери приватності (захисту персональних даних), кібератак в контексті міждержавних протистоянь, війн, втягненням неповнолітніх та інших осіб у кримінально протиправну діяльність, тероризм, виготовлення порнографії тощо. Сексуальний примус і здирство в Інтернеті є одним із нових кримінальних феноменів цифрових технологій. Сьогодні багато в чому завдяки популяризації соціальних медіа правопорушникам легше ділитися нелегальним вмістом і створювати його. Сексуальна експлуатація або насильство над дітьми в Інтернет виявляються одним з провідних сучасних трендів відтворення злочинності. Доведено, що кіберзлочинність є специфічним кримінально-комунікативним феноменом, що онтологізується через апаратне та програмне забезпечення, спрямовується на досягнення цілей, які здебільшого формуються поза кіберпростором, але реалізуються його засобами.

Ключові слова: кіберзлочин, кіберзлочинність, кримінальне правопорушення, девіація, злочинність, кіберпростір, цифрове середовище, шахрайство, порнографія, війна, кібератака.

Постановка проблеми. Шкідливе програмне забезпечення вражає мільйони домогосподарств, а загальний обсяг банківського шахрайства, пов'язаного з кіберзлочинністю, зростає з року в рік. Кіберзлочинність може знизити загальну довіру громадян до роздрібної торгівлі в Інтернеті, банківського сектору, держави загалом. Втрата впевненості в безпеці електронної комерції має прямий вплив на функціонування бізнесу. В умовах же протистояння збройній агресії з боку російської федерації Україна має зміцнювати як захищеність об'єктів, що мають оборонне значення, так і бізнесу. Первинним кроком на цьому шляху є осягнення змісту, специфіки феномену кіберзлочинності.

Окремі проблеми протидії кіберпросторі в Україні та світі досліджували такі вчені-юристи, як О. М. Кравцова, О. В. Манжай, Д. В. Пашнев, О. С. Передерій, В. В. Сокурєнко, К. О. Черевко та інші, які обґрунтовують необхідність розмежовування природи та проявів злочинності взагалі та кіберзлочинності, зокрема.

Мета статті полягає у визначення кримінологічно-феноменологічної природи кіберзлочинності.

Виклад основного матеріалу. А. П. Закалюк слушно, на нашу думку, зауважував, що злочинність – феномен суспільного життя у виді неприйнятної та небезпечної для суспільства масової, відносно стійкої, різнообумовленої кримінальної активності частини членів цього суспільства¹. При цьому предметно-сутнісне визначення злочинності через категорію суспільно неприйнятної активності потрібно не лише у суто теоретичних цілях. Воно має важливе методологічне значення. Саме через «олюднення» поняття злочинності у кримінології має реалізуватися соціально-антропологічний метод, якому тривалий час не знаходилося місця у радянській науці². В свою чергу О. М. Бандурка та О. М. Литвинов наголошують що – злочинність в соціальному і психологічному аспектах постає передусім як продукт діяльності людини, результат її соціальної активності і виявляється в масових повсякденних практиках, які можна позначити терміном «кримінальні практики»³.

Отже, перш за все злочинність є феноменом, а не явищем суспільного життя, тобто є не лише вираження через статистичну проявленість кримінальних правопорушень, вчинених на певній території за певний проміжок часу. Крім того, заслуговує на підтримку й подальший розвиток визначення онтологічного виміру інституціональної теорії злочинності. В цьому контексті аргументованою є позиція професора В. М. Дрьоміна, який вказує на те, що злочинність в реальному житті постає як різновид соціальної практики, що реалізується в конкретній предметній діяльності. В силу характеру та спрямованості цієї діяльності вона кваліфікується як злочинна діяльність, що дозволяє її віднести до такого різновиду соціальних практик, яку ми називаємо кримінальними практиками. Кількісні і якісні показники кримінальних практик свідчать про процеси їх інституціоналізації⁴.

Викладені положення щодо поняття злочинності є цілком обґрунтованими та прийнятними для оперування ними в нашому дослідженні. З них, серед іншого, випливає кілька важливих висновків щодо родових ознак злочинності в кіберсфері, кіберпросторі, тобто кіберзлочинності. По-перше, злочинність має соціально-діяльнісну феноменологічну природу. По-друге, вона має юридичний характер, що полягає у забороненій законом про кримінальну відповідальність діяльності певної частини населення – соціальних практиках. Змістовні характеристики останніх виявляють специфічні риси кіберзлочинності, що відрізняють її від інших суміжних кримінальних феноменів, суспільно небезпечних практик.

¹ Закалюк А. П. Курс сучасної української кримінології : теорія і практика : у 3-х кн. Кн. 1. К. : Видавничий Дім «Ін Юре», 2007. С. 139

² Там само. С. 139

³ Бандурка О. М., Литвинов О. М. Злочинність як об'єкт феноменологічного аналізу. *Право і безпека*. 2015. № 3. С. 6–10.

⁴ Дрьомін В. М. Інституціональна теорія злочинності та криміналізації суспільства : дис. ... докт. юрид. наук : 12.00.08 / Одеська національна юридична академія. Одеса, 2010. 422. С. 116.

Для більш детального з'ясування змісту досліджуваного поняття слід неодмінно звернути увагу й на ту обставину, що альтернативою йому в різних дослідженнях є такі, як «комп'ютерна злочинність», «злочини у кіберпросторі», «злочини у сфері інформаційних технологій», «електронний злочин», «цифровий злочин», «інтернет-злочин», «мережевий злочин» та «ІТ-злочин». Вибір конкретного виразу залежить від контексту та акценту, який потрібно зробити. Наприклад, «комп'ютерний злочин» може підкреслювати використання комп'ютера як інструменту, а «злочин у кіберпросторі» – середовище, де відбувається злочин. Зокрема, О. О. Загуменний доходить висновку, що термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі, але все-таки не синонімічні. Поняття «кіберзлочинність» (в англomовному варіанті – *cybercrime*) ширше, ніж «комп'ютерна злочинність» (*computer crime*), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі¹.

Проте, на наш погляд, всі перераховані нами терміни є синонімічними, а отже в цьому дослідженні ми будемо використовувати їх на рівні із терміном «кіберзлочинність». Такий підхід пояснюється наступними міркуваннями.

По-перше, серед авторів часто переважає думка, що кіберзлочинами є такі, що об'єднані специфічним місцем їх вчинення – кіберпростором. Відповідно, і визначення даються виходячи із цього: «Кіберзлочинність – це сукупність злочинів, що вчиняються в кіберпросторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до кіберпростору, в межах комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних»².

Таке розуміння кіберзлочинності викликає зауваження, тому що використовує за основу термін «кіберпростір», загально прийнятого значення якого також на даний момент не існує. На підтвердження цього проаналізуємо публікацію, яка містить достатню кількість визначень кіберпростору та може бути основою для певних висновків³.

Так, Т. В Федоренко та В. В. Федоренко наводять низку визначень кіберпростору відповідно до: 1) міжнародного стандарту ISO/IEC 27032: 2012 (*Information technology – Security techniques Guidelines for cybersecurity*) – це середовище існування, отримане у результаті взаємодії людей, програмного забезпечення, інтернет сервісів і послуг в Інтернеті за

¹ Загуменний О. О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини» // Процесуальне та техніко-криміналістичне забезпечення досудового розслідування : Зб. тез доп. всеукр. наук.-практ. конф. (м. Харків, 28 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2019. С. 69.

² Протидія кіберзлочинності в Україні : правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. К. : Скіф, 2012. С. 46.

³ Федоренко Т.В., Федоренко В.В. Основні положення кіберпростору: поняття та сутність. *Modern scientific journal*. 2023. Вип. 2 (2). С. 68-72. DOI: <https://doi.org/10.36994/2786-9008-2023-2-9>.

допомогою технологічних пристроїв і мережевих зв'язків, підключених до них, яке не існує у будь-якій фізичній формі;¹ 2) нормативної бази США – це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру; 3) офіційних документів Євросоюзу – це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК)²; 4) офіційних документів Великобританії – це всі форми мережевої, цифрової активності, що включають у себе контент та дії, які здійснюються через цифрові мережі³; 5) офіційних документів Німеччини – це вся інформаційна інфраструктура, що доступна через Інтернет поза будь-якими територіальними кордонами; 6) «Стратегії забезпечення кібернетичної безпеки України» – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем⁴.

З цього можна зробити висновок, що при всьому різноманітті цих визначень, при чіткій вказівці на пов'язаність кіберпростору з ІКТ інфраструктурою, основна увага звертається не на технології, а саме на діяльність людей, які використовують ці технології.

Теж саме запропонував і О. В. Манжай: «Кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами»⁵. З цього можна зробити висновок, що Т. В. Федоренко, В. В. Федоренко та О. В. Манжай, як і багато інших фахівців⁶, ідентифікує кіберпростір із певним *єдиним* простором, створеним всіма засобами комп'ютерних технологій. І маються на увазі всі мережі, об'єднані мережею Інтернет. Але за такого підходу до категорії кіберзлочинів не потрапляють кримінальні правопорушення, вчинені в локальній мережі, не приєднаній до Інтернет, не кажучи вже про локальний комп'ютер, що не може задовольнити запити нашого дослідження у формуванні повного поняття кіберзлочинності.

На це питання відповів П. М. Сніцаренко, вказавши таке: «...Розглядати і визначати кіберпростір як віртуальне середовище – помилка, якої не

¹ Information technology – Security techniques – Information security management systems : ISO/IEC 27001:2005 –Requirements. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en>.

² European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). URL: <http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm>.

³ Cyberspace // Oxford English Dictionary. URL: https://www.oed.com/dictionary/cyberspace_n?tl=true.

⁴ Федоренко Т.В., Федоренко В.В. Основні положення кіберпростору: поняття та сутність. *Modern scientific journal*. 2023. Вип. 2 (2). С. 70. DOI: <https://doi.org/10.36994/2786-9008-2023-2-9>.

⁵ Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека*. 2009. № 4 (31). С. 216.

⁶ Krock R. An Internet Connection does not equal Internet access. *ICT Works*. 2014. URL: <https://www.ictworks.org/an-internet-connection-does-not-equal-internetaccess/>.

можна допускати. Інше питання ставиться під сумнів контекстуальним твердженням, що кіберпростір охоплює лише глобальні комп'ютерні мережі. Підозра викликана наявністю реальних процесів електронного зв'язку не тільки в глобальних, але і в різних ізольованих локальних комп'ютерних мережах...».¹

Все ж таки ми не відповіли на питання щодо одного комп'ютера, операційної системи, чи може вона визнаватися кіберпростором. На це є відповідь – ні. Така мережа без тематичного інформаційного наповнення є просто «металевою» структурою, яка має обсяг, вагу та технічну можливість комп'ютерів взаємодіяти

Іншими словами, щоб краще зрозуміти, які кримінальні правопорушення слід вважати кіберзлочинами, варто почати з того, що означають слова «кібер» та «злочинність» окремо. Префікс «кібер» (cyber – такий, що походить від cybernetics) додають до повсякденних слів, щоб показати їхню причетність до Інтернету, комп'ютерів тощо. А кібернетику (cybernetics (від грец. cybernos – рульовий)) зараз розглядають як науку про зв'язки, управління й організацію в об'єктах різноманітної природи².

Простіше кажучи, навіть якщо ми лише поверхово розглянемо слово «кіберзлочинність» стає зрозуміло, що головне, що об'єднує всі його значення, – це використання інформаційних технологій та засобів зв'язку. Ці технології по-різному застосовуються при вчиненні кримінальних правопорушень, які є предметом вивчення цієї сфери, а також часто повторюються в реальному житті. Очевидно, що для вчинення таких кримінальних правопорушень використовуються комп'ютери, системи зв'язку та Інтернет. Проте, навіть розуміння цього недостатньо, щоб точно визначити, що саме відноситься до кіберзлочинності.

Слово «кіберзлочинність» почали офіційно використовувати в Україні після того, як країна підписала міжнародну угоду про боротьбу з такими злочинами, а саме Будапештську конвенцію³ та додатковий протокол до цієї Конвенції⁴, яка є першим міжнародним договором, спрямованим на боротьбу з кіберзлочинністю. Але ця угода не дає чіткого визначення, що саме вважається «кіберзлочином», а лише перелічує різні види порушень, які до нього належать. Кримінальний кодекс України та інші закони також не мають точного визначення «кіберзлочинів». Тому, коли розробляються правила для визначення та класифікації цих злочинів, виникає питання, як

¹ Сніцаренко П., Саричев Ю., Гордійчук В. «Сутність кіберпростору та його взаємозв'язок із кібернетичним простором», *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2 (50). С. 5–10. DOI: 10.33099/2311-7249/2024-50-2-5-10.

² Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування / Е. М. Пройдаков, Л. А. Теплицький. К. : СофтПрес, 2005. С. 133–134.

³ Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575; Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 року № 2824-IV. URL: <http://zakon1.rada.gov.ua/laws/show/2824-15>.

⁴ Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Міжнародний документ (Рада Європи). Протокол від 28.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

відрізнити їх від інших видів кримінальних правопорушень, враховуючи всі їхні особливості. Вказані у цих міжнародних документах кримінальні правопорушення і повинні вважатися «кіберзлочинами».

Перш ніж продовжити треба розглянути та з'ясувати яке саме визначення поняття «кіберзлочинність» ми повинні використовувати. Так, А. В. Боровик та І. М. Копотун наполягають, що: «...семантичний аналіз поняття кіберзлочинності вказує на те, що інтегруючим елементом складників цього поняття є інформаційні-телекомунікаційні технології, які різним чином задіяні при вчиненні відповідних діянь. І взагалі основною сутнісною ознакою кіберзлочину є те, що це є діяння, сама можливість вчинення якого впливає з особливих можливості інформаційно-телекомунікаційних (комунікаційних) технологій, які використовуються для завдання шкоди суспільним відносинам...»¹. Для розуміння терміна «інформаційно-телекомунікаційна технологія» треба звернутися до Закону України «Про захист інформації в інформаційно-комунікаційних системах», у ст. 1 якого зафіксовано поняття інформаційно-комунікаційних систем – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле².

Іншої думки І. Д. Діордіца, який вказує, що кіберзлочин – це дії, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані або у систему; зловживання пристроям; шахрайство; правопорушення, пов'язані з дитячою порнографією; порушення авторських і суміжних прав; правопорушення, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, що тягнуть кримінальну відповідальність³.

З наведених визначень кіберзлочинності стає зрозуміло, що це поняття охоплює надзвичайно широке коло правопорушень. Способи їх класифікації та типології також є предметом жвавих наукових дискусій, у тому числі на міжнародному рівні. Іншими словами, якщо розглянути, як різні науковці в Україні вивчають та пояснюють, що таке «кіберзлочин», стає очевидно, що немає однієї спільної думки. Їхні погляди на це питання досить сильно різняться. А це, у свою чергу, може призвести до помилок у визначенні того, який закон застосовувати до таких дій. Через це можуть виникнути проблеми не лише в теорії, але й у практичній роботі правоохоронних органів та судів.

Висновок. Ми можемо зробити висновок, що кіберзлочинність є феноменом багатоплановим, складноутвореним. Незважаючи на різне функціональне навантаження різних практик, що його складають, всіх їх об'єднує те, що вони є по суті кримінально протиправною діяльністю, що

¹ Боровик А. В., Копотун І. М. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб. Луцьк : СПД Гадяк Ж. В. друкарня «Волиньполіграф» ТМ, 2019. С. 54.

² Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

³ Діордіца І. В. Поняття та зміст кіберзлочинності. *Науковий Вісник Херсонського державного університету. Серія: Юридичні науки*. 2017. № 3. Т. 2. С. 10.

здійснюється у цифровому просторі. Але сам цей простір, підкреслимо, є системою інструментів комунікації. І це є специфікою кіберзлочинності, що дає можливість її визначити як специфічний кримінально-комунікативний феномен, що онтологізується через апаратне та програмне забезпечення, спрямовується на досягнення цілей, які здебільшого формуються поза кіберпростором, але реалізуються його засобами. Таким чином цифровий інструментарій є лише провідником, комплексом умов відтворення кіберзлочинності, причини якої укорінені глибоко в соціальній матерії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування / Е. М. Проїдаков, Л. А. Теплицький. К. : СофтПрес, 2005. 546 с.
2. Бандурка О. М., Литвинов О. М. Злочинність як об'єкт феноменологічного аналізу. *Право і безпека*. 2015. № 3. С. 6–10.
3. Боровик А. В., Копотун І. М. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб. Луцьк : СПД Гадяк Ж. В. друкарня «Волиньполіграф» ТМ, 2019. 304 с.
4. Діордіца І. В. Поняття та зміст кіберзлочинності. *Науковий Вісник Херсонського державного університету. Серія: Юридичні науки*. 2017. № 3. Т. 2. С. 8–13.
5. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Міжнародний документ (Рада Європи). Протокол від 28.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.
6. Дрьомін В. М. Інституціональна теорія злочинності та криміналізації суспільства : дис. ... докт. юрид. наук : 12.00.08 / Одеська національна юридична академія. Одеса, 2010. 422 с.
7. Загуменний О. О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини» // Процесуальне та техніко-криміналістичне забезпечення досудового розслідування : Зб. тез доп. всеукр. наук.-практ. конф. (м. Харків, 28 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2019. С. 68–70.
8. Закалюк А. П. Курс сучасної української кримінології : теорія і практика : у 3-х кн. Кн. 1. К. : Видавничий Дім «Ін Юре», 2007. 424 с.
9. Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.
10. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека*. 2009. № 4 (31). С. 215–219.
11. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

12. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 року № 2824-IV. URL: <http://zakon1.rada.gov.ua/laws/show/2824-15>.
13. Протидія кіберзлочинності в Україні : правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. К. : Скіф, 2012. 728 с.
14. Сніцаренко П., Саричев Ю., Гордійчук В. «Сутність кіберпростору та його взаємозв'язок із кібернетичним простором», *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 2 (50). С. 5–10. DOI: 10.33099/2311-7249/2024-50-2-5-10.
15. Федоренко Т.В., Федоренко В.В. Основні положення кіберпростору: поняття та сутність. *Modern scientific journal*. 2023. Вип. 2 (2). С. 68-72. DOI: <https://doi.org/10.36994/2786-9008-2023-2-9>.
16. Cyberspace // Oxford English Dictionary. URL: https://www.oed.com/dictionary/cyberspace_n?tl=true.
17. Information technology – Security techniques – Information security management systems : ISO/IEC 27001:2005 – Requirements. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en>.
18. Krockner R. An Internet Connection does not equal Internet access. *ICT Works*. 2014. URL: <https://www.ictworks.org/an-internet-connection-does-not-equal-internetaccess/>

Стаття надійшла до редакції 18.11.2024

Petro P. GALUSHKO,

Postgraduate Student

(*Kharkiv National University of Internal Affairs, Kharkiv, Ukraine*)

CYBERCRIME IN THE FOCUS OF CRIMINOLOGY-PHENOMENOLOGICAL ANALYSIS

Cybercrime affects all segments of the population both in our country and in the world. The problem is most acute in the area of the spread of sheikhrays, violations of the sphere of privacy (protection of personal data), cyberattacks in the context of interstate confrontations, wars, involvement of minors and other persons in criminal and illegal activities, terrorism, production of pornography, etc. Sexual coercion and extortion on the Internet is one of the new criminal phenomena of digital technologies. It has been proven that cybercrime is a specific criminal-communicative phenomenon that is ontologized through hardware and software, aimed at achieving goals that are mostly formed outside cyberspace, but are implemented by its means.

Keywords: *cybercrime, cybercrime, criminal offense, deviation, crime, cyberspace, digital environment, fraud, pornography, war, cyberattack.*