

Діана КІРІКА,

кандидат юридичних наук, доцент,
доцент кафедри адміністративної діяльності ННІ №3
Харківського національного університету внутрішніх
справ м. Кам'янець-Подільський, Україна
ORCID: <https://orcid.org/0000-0002-3633-0103>,
e-mail: dkirika7@gmail.com

Вадим КІРІКА,

конкурсант МАН, учень Кам'янець-Подільського ліцею
№18 м. Кам'янець-Подільський, Україна

DOI: <https://doi.org/10.32620/pls.2025.8.16>

СОЦІАЛЬНО-ПРАВОВИЙ ФЕНОМЕН КІБЕРБУЛІНГУ ЯК ФОРМИ ПОРУШЕННЯ ПРАВ И СВОБОД ЛЮДИНИ

Анотація: Тези доповіді присвячені комплексному дослідженню соціально-правового феномену кібербулінгу як сучасної форми порушення прав і свобод людини. У роботі розкривається сутність кібербулінгу, його основні прояви та вплив на особистість у цифровому середовищі. Автори аналізують соціальні чинники, що сприяють поширенню цього явища, визначають ключові ризики для психологічного добробуту й безпеки користувачів, особливо дітей і молоді. У правовому аспекті висвітлюються національні та міжнародні підходи до регулювання кібербулінгу, окреслюються прогалини законодавства та пропонуються шляхи удосконалення правових механізмів захисту. Особливу увагу приділено ролі державних інституцій, освітніх закладів та інтернет-платформ у попередженні й протидії кібербулінгу.

Ключові слова: інформаційна сфера, права і свободи, булінг, кібербулінг, кіберзлочинність, фішинг, кібербулери, відповідальність.

Сьогодні інформаційна сфера є однією з найбільш динамічних і стрімко розвиваючих сфер суспільних відносин, яка потребує належного правового регулювання. Ставши невід'ємною частиною життя сучасного суспільства, Інтернет породив нове явище під назвою кіберпростір. Однак дана сфера стала і ідеальним підґрунтям для злочинців, що діють у віртуальному просторі, завдаючи великої шкоди не тільки державним інституціям, а й окремим громадянам. Стрічки інформаційних ресурсів та соціальних мереж все більше наповнюються історіями про цькування дітей та молоді через Інтернет, що нерідко призводить до страшних чи навіть фатальних наслідків. Кіберзлочинність стала реальною загрозою сучасного суспільства. За статистикою в Україні зростає кількість дитячих та підліткових суїцидів. За даними Єдиного досудового реєстру за рік в середньому вчиняється понад 120 випадки підліткових самогубств, причиною яких часто називають кібербулінг [1].

У 2019 році до Закону України «Про освіту» [2] було внесено поняття «булінгу», однак воно насамперед було орієнтоване на шкільне середовище та не охоплювало повний спектр онлайн-насилюства, що може відбуватися поза закладом освіти (у соцмережах, месенджерах, ігрових платформах тощо). Стрімке поширення

цифрових технологій спричинило появу нових проявів протиправної поведінки, серед яких особливе значення має кібербулінг. Збільшення випадків онлайн-цькування, психологічного тиску та приниження, зокрема серед дітей і підлітків, підкреслює потребу в удосконаленні правових інструментів протидії таким явищам. Так, Закон «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» [3], який набрав чинності також у 2019 році, включав поняття булінгу із застосуванням засобів електронних комунікацій (тобто кібербулінг). Однак українське кримінальне законодавство так і не дає окремого загального визначення терміну «кібербулінг» у відношенні повнолітніх осіб - тобто немає прямої статті, що окреслює окреме правопорушення саме «кібербулінгу» поза освітнім контекстом.

Очевидним є те, що кібербулінг і прямо, і опосередковано порушує низку фундаментальних прав людини, оскільки завдає психологічної шкоди, обмежує свободи та створює небезпечне середовище для особи. Основні права, які можуть бути порушені: право на гідність та недоторканність честі, право на приватність, право на свободу від насильства та жорстокого поводження, право на свободу вираження поглядів (у безпечному середовищі), право на освіту, право

на здоров'я, право на безпеку та інші права людини.

Розглянемо ці права більш детально, з точки зору загроз, які несе в собі кібербулінг.

Статті міжнародних документів (наприклад, Загальної декларації прав людини) гарантують повагу до честі й гідності особи [4]. Кібербулінг принижує людину, поширює образи, наклепи та дискредитує інформацію - усе це є прямим посяганням на її гідність та честь. Поширення приватних фото, відео, особистої інформації, доксинг - пряме порушення права на приватне життя. Кібербулінг часто включає небажане стеження, злам акаунтів, витік персональних даних. Психологічний тиск, переслідування, погрози, залякування в Інтернеті можуть розглядатися як форма психологічного насильства. Коли людину переслідують за її висловлювання, цькують у соцмережах, створюють хвилі хейту, це обмежує свободу слова, змушуючи мовчати через страх. Учні та студенти, які зазнають кібербулінгу, часто перестають відвідувати навчання або не можуть повноцінно навчатися через стрес та страх, що порушує їх право на доступ до освіти. Кібербулінг призводить до стресу, тривожності, депресії, психосоматичних розладів - тобто порушує право на найвищий досяжний рівень фізичного та психічного здоров'я. Погрози, розправи, публікація адреси, переслідування онлайн можуть створювати реальну загрозу життю й свободі людини, призводити до порушення права на особисту безпеку людини.

Ключовими характеристиками кіберзлочинності є її глобальність, анонімність та висока динамічність розвитку. Злочинці можуть діяти з будь-якої точки світу, використовуючи технічні засоби для приховування своєї особистості, а методи нападу постійно змінюються та удосконалюються. Кібербулінг відбувається в Інтернеті, переважно через соціальні мережі, месенджери та ігрові платформи. Інтернет-цькування або кібертравля - це навмисні образи, погрози, дифамації і повідомлення іншим компрометуючих даних за допомогою сучасних засобів комунікації, як правило, протягом тривалого періоду часу [5]. Жертви кіберзалякування можуть відчувати серйозні емоційні та психологічні наслідки, включаючи депресію та тривогу. Анонімність Інтернету часто дозволяє зловмисникам діяти безкарно, що ускладнює боротьбу з цією проблемою.

Важливо розглянути основні види кіберзлочинів, які не тільки порушують права людини, але й несуть потенційні загрози і її здоров'ю (психологічному, емоційному, фізіологічному), можуть включати психологічну травму жертви, зниження якості життя, а в деяких випадках і самогубство.

Хакерство або несанкціонований доступ передбачає проникнення до інформаційних систем, серверів або акаунтів користувачів з метою викрадення, зміни або знищення даних. Хакери можуть використовувати вразливості програмного забезпечення, соціальну інженерію чи підбір паролів (brute-force). Комп'ютерне

шахрайство включає в себе фінансові махінації, обман або маніпуляції з використанням електронних систем. Це можуть бути крадіжки грошей через онлайн-банкінг, інвестиційні афери, продаж фіктивних товарів або послуг. Розповсюдження шкідливого програмного забезпечення (віруси, трояни, ransomware), метою яких є виведення систем з ладу, блокування доступу до даних, збір конфіденційної інформації або навіть шантаж (наприклад, віруси-шифрувальники). Фішинг - спроба виманити в користувачів конфіденційні дані - логіни, паролі, номери банківських карток шляхом створення фальшивих веб-сайтів, електронних листів або повідомлень, що маскуються під офіційні джерела. Онлайн-переслідування здійснюється шляхом образи, погрози, поширення неправдивої чи приватної інформації, маніпулювання, приниження в соцмережах і месенджерах, що є особливо небезпечним через швидкість поширення інформації та можливість анонімності агресора. Компрометація персональних даних можлива шляхом викрадення або незаконного використання даних користувачів (адрес та номерів телефонів, паспортної інформації, медичних записів, фінансових документів) та інші види.

Єдиний підхід до класифікації видів кібербулінгу у науковців відсутній. Деякі з них не виділяють основні та додаткові види, а ставлять їх усі поряд, інші - об'єднують схожі за своєю суттю поняття у групи, або зазначають, що окремі з них впливають з попередніх [6, с. 145]. Наслідками кібербулінгу, через розглянуті правопорушення, стають фінансові збитки для громадян, порушення роботи сервісів, ризики витоку конфіденційної інформації, психологічний тиск, страх, стрес і травматичні наслідки.

Кібербулери та хейтери - це особи, які навмисно принижують, ображають, погрожують, переслідують, критикують («хейтять») інших у мережі. Вони використовують цифрові платформи, такі як: соціальні мережі (Instagram, TikTok, Facebook), месенджери, онлайн-ігри, електронну пошту, форуми та чати. Свій агресивний контент хейтери виражають у формах: образ, глузування, приниження, поширення брехні або чуток, публікації приватної інформації без дозволу, створення фейкових акаунтів для цькування, надсилання погроз чи агресивних повідомлень, пишуть неприємні коментарі, але не завжди мають на меті довготривале переслідування. Їхня поведінка може бути грубою, неповагою, токсичною. Їхня мета завдати шкоди та психологічного болю, довести людини до стресу чи страху, тому їх кібербулінг набуває характеру тривалої агресії.

Спробуємо окреслити види та межі відповідальності, передбачені законодавством щодо реагування на розглянуті вище факти кібербулінгу.

Юридичні ініціативи щодо захисту від кіберзагроз відіграють важливу роль у забезпеченні безпеки в цифровому просторі. Багато країн розробляють і впроваджують закони для боротьби з кіберзлочинністю, включно з

кримінальними законами, які охоплюють такі злочини, як хакерство та викрадення особистих даних. Міжнародні угоди, такі як Конвенція про кіберзлочинність, заохочують співпрацю між державами у розслідуванні та судовому переслідуванні кіберзлочинців.

Стаття 173-4 Кодексу України про адміністративні правопорушення (далі - КУпАП) передбачає відповідальність за булінг (цькування) учасника освітнього процесу, включно з діями через електронні засоби (соцмережі, месенджери тощо). Санкції даної статті передбачають: штраф від 50 до 100 НМДГ (орієнтовно 850–1700 грн); громадські роботи від 20 до 40 год.; посилена відповідальність, якщо правопорушення вчинено групою осіб чи повторно [7]. У випадку неповідомлення про випадки булінгу в навчальному закладі, для його керівника передбачений штраф. Якщо булінг вчиняють діти 14–16 років, навантаження відповідальності покладається на батьків.

Прямої статті Кримінального кодексу України (далі – ККУ) за сам факт кібербулінгу як окремого кримінального правопорушення немає. Проте кримінальна відповідальність може наставати залежно від наслідків протиправних дій, а саме: стаття 120 ККУ «Доведення до самогубства» передбачає позбавлення волі, якщо цькування призвело до спроби або факту самогубства [8]. Погроза вбивством, тяжкі тілесні ушкодження теж застосовуються до протиправних дій кібербулерів, якщо вони підпадають під ознаки складу цих кримінальних правопорушень, а не як окрема стаття про «кібербулінг».

Якщо кібербулінг супроводжується поширенням неправдивої інформації, порушенням честі та гідності особи, потерпілий може звертатися до суду на підставах ст.ст. 277–280 Цивільного кодексу України (далі – ЦКУ) [9] з вимогою про спростування недостовірної інформації, захисту честі, гідності та ділової репутації. Це важливий додатковий спосіб правового реагування за відсутності загальної кримінальної статті про кібербулінг.

Органи поліції, зокрема кіберполіція [10], проводять інформаційні кампанії, консультують про реагування та захист у випадках кібербулінгу. Освіта є важливим фактором у підвищенні обізнаності про кіберзагрози, оскільки вона допомагає людям зрозуміти ризики, пов'язані з використанням технологій. Це допоможе молодому поколінню зрозуміти ризики та навчитися захищати свої дані. Програми навчання кібербезпеці можуть сприяти безпечнішій поведінці в Інтернеті, навчаючи користувачів розпізнавати фішинг, зловмисне програмне забезпечення та інші загрози. Крім того, навчальні ініціативи можуть сприяти розвитку культури безпеки, у якій кожен розуміє свою роль у захисті особистої та корпоративної інформації. Тому інвестиції в освіту з кібербезпеки можуть значно зменшити кіберзагрози та підвищити загальну безпеку суспільства.

Кібербулінг трактується як агресивну, систематичну поведінку в мережі з елементами навмисності, повторюваності та нерівності сил.

Кіберзлочинність стала однією з найсерйозніших загроз сучасному суспільству та впливає на всі аспекти життя - від бізнесу до особистої безпеки громадян. В Україні вже існують певні норми, що регулюють це питання, міжнародна практика пропонує різноманітні підходи, корисні для подальшого запозичення. Загальна правова норма про кібербулінг як окремий злочин чи правопорушення ще не сформована, і тому потерпілі часто користуються суміжними механізмами захисту. Українське законодавство частково регулює протидію кібербулінгу: прямо - у контексті освітнього процесу через адміністративну відповідальність; опосередковано - через кримінальне та цивільне право за наслідки протиправних дій; захисні механізми працюють, але мають вузький та локалізований характер.

Виходячи з вищевикладеного, кіберзлочинність представляє собою комплекс усіх видів протиправних дій, що здійснюються за допомогою комп'ютерних систем, мобільних пристроїв, мережевих технологій та Інтернету. Вона охоплює широкий спектр правопорушень, які загрожують безпеці інформації, фінансовим ресурсам, приватному життю користувачів, а також стабільному функціонуванню суспільства в цілому. Увага повинна зосереджуватись на комплексному підході до проблеми кібербулінгу та необхідності спільних зусиль усіх зацікавлених сторін для створення безпечного онлайн-середовища.

Бібліографічні посилання

1. Протидія кібербулінгу: суб'єкти реагування та механізми захисту порушених прав дитини. URL: <https://www.hsa.org.ua/blog/protydiya-kiberbulingu-sub-yekty-reaguvannya-ta-mehanizmy-zahystu-porushenyh-prav-dytyny>
2. Про освіту : Закон України від 05.09.2017 № 2145-VIII // База даних «Законодавство України» / Верховна Рада України. — Режим доступу: <https://zakon.rada.gov.ua/go/2145-19> (дата звернення: 06.12.2025)
3. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) : Закон України від 18.12.2018 № 2657-VIII // База даних «Законодавство України» / Верховна Рада України. — Режим доступу: <https://zakon.rada.gov.ua/go/2657-19> (дата звернення: 06.12.2025)
4. Загальна декларація прав людини прийнята і проголошена резолюцією 217 A (III) Генеральної Асамблеї ООН від 10 грудня 1948 року URL: https://zakon.rada.gov.ua/laws/show/995_015/print (дата звернення: 06.12.2025).
5. Кібермоббінг // Вікіпедія : віл. енцикл. URL: <https://uk.wikipedia.org/wiki/Кібермоббінг>
6. Пилипишина І.І. Протидія кібербулінгу як забезпечення права дитини на безпеку. Науковий вісник Ужгородського Національного Університету, 2024. С. 142-149.
7. Кодекс України про адміністративні правопорушення : від 07.12.1984 № 80731-10 // База даних «Законодавство України» / Верховна Рада України. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 07.12.2025)

8.Кримінальний кодекс України від 05.04.2001 № 2341-III. - URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 08.11.2025).

9.Цивільний кодекс України : від 16.01.2003 № 435-IV // База даних «Законодавство України» / Верховна Рада України. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 08.12.2025)

10.Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: <https://www.google.com/url?sa=E&source=gmail&q=https://zakon.rada.gov.ua/laws/show/580-VIII> (дата звернення: 24.11.2025).

D. Kirika, V. Kirika

The socio-legal phenomenon of cyberbullishing as a forms of violation of human rights and freedoms.

Abstract: The abstracts of the report are devoted to a comprehensive study of the socio-legal phenomenon of cyberbullying as a modern form of violation of human rights and freedoms. The work reveals the essence of cyberbullying, its main manifestations and impact on the individual in the

digital environment. The authors analyze the social factors that contribute to the spread of this phenomenon and identify key risks to the psychological well-being and safety of users, especially children and young people. The legal aspect highlights national and international approaches to regulating cyberbullying, outlines gaps in legislation, and suggests ways to improve legal protection mechanisms. Special attention is paid to the role of state institutions, educational institutions, and Internet platforms in preventing and combating cyberbullying.

Keywords: information sphere, rights and freedoms, bullying, cyberbullying, cybercrime, phishing, cyberbullies, responsibility.

Зразок для цитування:

Кіріка Д., Кіріка В. Соціально-правовий феномен кібербулінгу як форми порушення прав и свобод людини. Пропілеї права та безпеки, 2025. №8. С. 88-91. DOI: <https://doi.org/10.32620/pls.2025.8.16>.