Рябокінь Максим Русланович,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРБУЛІНГ В УКРАЇНІ: ФОРМИ, СОЦІАЛЬНО-ПСИХОЛОГІЧНІ НАСЛІДКИ ТА ПРАВОВЕ РЕГУЛЮВАННЯ

Проблема кібербулінгу, є однією з найбільш гострих соціальних та правових загроз, що виникають внаслідок стрімкої інтеграції цифрових технологій у повсякденне життя. Кібербулінг визначається як форма психологічного насильства, що здійснюється із застосуванням електронних комунікаційних технологій [1]. Інше поширене визначення трактує його як агресивний, навмисний вчинок, що здійснюється групою або індивідом за допомогою електронних засобів зв'язку, повторювано і з часом, проти жертви, яка не може легко захистити себе [2]. Саме така повторюваність та доступність цифрових платформ робить кібербулінг особливо небезпечним.

Масштаби кібербулінгу в Україні, за даними національних та міжнародних досліджень, є тривожними: щонайменше третина підлітків у віці 12–18 років засвідчували або ставали жертвами цькування в мережі [3]. Така висока поширеність обумовлена постійною доступністю Інтернету, зниженням рівня цифрового етикету та недостатньою обізнаністю користувачів. Основні платформи, що використовуються для цькування, включають соціальні мережі (Instagram, TikTok), месенджери (Telegram), а також онлайн-ігри та електронну пошту.

Цифрове середовище надає агресорам можливість анонімності та необмеженого поширення інформації, що багаторазово посилює психологічний тиск на жертву.

Серед основних форм кібербулінгу виділяють:

1. Тролінг (Trolling) – систематичне розміщення провокаційних або образливих повідомлень з метою емоційного розпалювання конфлікту [4]. Наприклад, навмисне провокування конфлікту у коментарях під відео.

2. Кіберсталкінг (Cyberstalking) або переслідування – залякування та збір особистої інформації про жертву (фото, геолокація) з подальшою розсилкою погроз або принизливих повідомлень, що часто має тривалий і нав'язливий характер [4].

3. Поширення конфіденційних даних (Doxing та Impersonation) –розголошення особистої інформації жертви без її згоди (Doxing) або видавання себе за іншу особу шляхом створення фейкових облікових записів для дискредитації чи зловживання довірою (Impersonation) [4].

4. Виключення (Exclusion) – навмисне виключення особи з онлайн-групи, чату чи спільноти з метою соціальної ізоляції [5].

5. Кіберхарасмент (Cyberharassment) – неодноразове надсилання образливих, ворожих або загрозливих повідомлень [5].

6. Хепі-слепінг (Happy Slapping) – акт насильства (фізичного або морального приниження) із записом на камеру та публічним розповсюдженням відео у мережі [5].

Кібербулінг часто межує з іншими кримінальними діяннями. До них належать:

1. Кібершантаж (Cyber Extortion) – вимагання грошей чи інших благ під загрозою розповсюдження компрометуючих даних або відео [4]. Наприклад, погрози опублікувати приватні фото, якщо жертва не виконає вимоги.

2. Фінансовий аб'юз онлайн (Online Financial Abuse) – несанкціоновані транзакції, злом акаунтів або вимагання грошей через цифрові платформи [4].

3. Несанкціоноване втручання у цифрові системи – злом облікових записів, серверів чи банківських систем з метою крадіжки фінансової чи персональної інформації [4].

Наслідки кібербулінгу для жертв є глибокими та деструктивними. Публічність та повторюваність цькування призводять до депресії, підвищеної тривожності, порушень сну, соціальної ізоляції, апатії до навчання та, в крайніх випадках, до формування суїцидальних думок [6]. Це руйнує інтегративний характер соціального середовища, підкреслюючи необхідність комплексних превентивних заходів.

В Україні правове регулювання кібербулінгу ще перебуває на стадії формування. На відміну від західних країн, де антибулінгова політика підкріплена чітким законодавством, в Україні досі відсутній спеціальний закон, що визначав би поняття «кібербулінг» та класифікував його форми. Це ускладнює процеси збирання доказів та притягнення винних до відповідальності.

Наразі застосовуються такі правові механізми:

1. Кодекс України про адміністративні правопорушення: Стаття 173-4 (Булінг/цькування), яка охоплює і кібербулінг, але не деталізує його специфіку [7].

2. Кримінальний кодекс України: Статті 120 (доведення до самогубства), 129 (погроза вбивством) та 301 (розповсюдження інтимних зображень без згоди) [7].

3. Закон України «Про освіту» (ст. 25, 26): Регулює запобігання булінгу в освітньому середовищі [7].

Боротьба з кібербулінгом ускладнюється безкарністю та браком чіткої відповідальності за дії в мережі. Необхідне термінове доопрацювання законодавства, що регламентує відповідальність за кібербулінг, сприяючи ефективнішій роботі Кіберполіції та судових органів. Паралельно важливим є впровадження освітніх програм для учнів та педагогів, спрямованих на підвищення цифрової грамотності, формування культури цифрового етикету та створення доступних механізмів подання скарг для жертв. Лише комплексний підхід, що поєднує правову регламентацію та просвітницьку діяльність, здатен забезпечити безпечне цифрове середовище.

Список використаних джерел

1. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: Bullying in the digital age (2nd ed.). Wiley-Blackwell.

2. Patchin, J. W., & Hinduja, S. (2013). Cyberbullying. , The Encyclopedia of Criminology and Criminal Justice. Wiley-Blackwell.

3. Денісова, А. (2021). Кібербулінг: поширеність та наслідки в учнівському середовищі.

4. Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. Journal of Politeness Research, 6(2), 215–242.

5. Willard, N. E. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Center for Safe and Responsible Internet Use.

6. Hinduja S., Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), 206–221.

7. Законодавчі акти України: Кодекс України про адміністративні правопорушення, Кримінальний кодекс України, Закон України «Про освіту».

Саінчин Олександр Сергійович,
професор кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

КРИМІНАЛІСТИЧНІ ЗАСАДИ ПРОТИДІЇ КРИМІНАЛЬНОГО ПРАВА В КІБЕРПРОСТОРІ

Стратегія інформаційної безпеки України – це державний документ, що визначає загрози, стратегічні цілі та завдання для захисту інформаційної сфери держави. Її головна мета – забезпечити захист життєво важливих інтересів громадян, суспільства та держави, протидіяти загрозам, забезпечувати суверенітет, територіальну цілісність та права громадян. Документ затверджений указом Президента № 685/2021 від 28 грудня 2021 року, реалізація якого розрахована до 2025 року [1; 2].

Згідно з затвердженим Кабінетом Міністрів плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року визначні наступні стратегічні цілі, на деяких аспектах реалізації яких в контексті служби безпеки України, ми вважаємо доцільно зупинитися окремо [3]:

1. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини і громадянина.