УДК 340.13:343.41(045)

М. М. Новіков,
кандидат юридичних наук, доцент

М. М. Новікова,
кандидат юридичних наук, доцент
ORCID ID: https://orcid.org/0000-0002-0334-3979

ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ КІБЕРНАСИЛЬСТВА: ПОНЯТТЯ ТА ЗМІСТ

Херсонський факультет Одеського державного університету внутрішніх справ
вул. Фонвізіна, 1, 73000, Херсон, Україна
E-mail: novikovamariia1222@gmail.com

Мета: *здійснити аналіз теоретичних аспектів кібернетичного насильства як одного із суспільно небезпечних проявів впливу на суспільство.* ***Методами дослідження*** *виступають загальнонаукові та спеціальні методи наукового пізнання, серед яких діалектичний метод, методи формальної логіки, структурно-логічний метод, категоріальний та ін.* ***Результати:*** *визначено, що подолання кібернасильства в Україні потребує формування системи комплексних заходів. У першу чергу, це стосується створення належного механізму правового регулювання, який чітко визначатиме правовий статус органів і підрозділів, які займатимуться питанням протидії кібернасильству.* ***Обговорення:*** *встановлено, що провідними засобами кібернасильства є виявлення і здійснення протягом певного часу стосовно чітко визначеного кола осіб психічного, біологічного, сексуального, фізичного, майнового, економічного, фінансового та інших видів насильства з використанням комп'ютерної техніки, кібернетичних (загальних та локальних) комп'ютерних мереж. Підкреслено, що кібернасильство спрямоване на пригнічення свідомості та волі осіб, які найчастіше мають активну соціальну позицію з боку осіб, схильних до девіантної поведінки. Поведінка останніх спрямована на дестабілізацію суспільства та держави, моралі, приниження загальнолюдських цінностей.*

У статті зроблено висновок, що більшість проявів кібернасильства вчинюється у молодіжному середовищі, якому притаманний низький рівень суспільної моралі та культури, а також правової обізнаності. Згідно даних UNICEF, в Україні близько 50% підлітків були жертвами кібернасильства. Встановлено, що в Україні нещодавно почала приділятися увага профілактиці кібернасильства серед неповнолітніх (кібербулінгу). Однак, правове регулювання даної сфери та здійснення захисту з боку держави залишається мінімальним. Введення в дію норми, яка визначає адміністративну відповідальність за булінг учасника освітнього процесу, не дає необхідного захисту дійсному колу потерпілих осіб від кібернасильства. При цьому визначено, що статистичних даних щодо кібернасильства у бік дорослої частини населення України немає. Це свідчить про латентність психологічного цькування, яке розгортається у соціальних мережах, мессенджерах, інтернет-сайтах.

Ключові слова: *кібернасильство; кіберзлочинність; булінг; цькування.*

Постановка проблеми та її актуальність. Із розвитком інформаційного простору та доступністю інтернет-технологій все більшої уваги привертає питання кібернасильства, яке набуває загрозливих масштабів на фоні майже повної безкарності. За даними Комітету цифрової трансформації України понад 18% рішень щодо булінгу, які зібрані відповідно до Єдиного

реєстру судових рішень, винесені щодо дій, які були здійснені через мережу Інтернет [1]. При цьому, не викликає навіть сумнівів те, що ці 18% стосуються лише випадків, коли потерпілі або не побоялися домогтися справедливості, або мали достатньо інформації про правопорушника. Вважаємо, що при аналізі самого явища можна говорити про його латентність, яка характеризується замовчуванням випадків правопорушень з боку потерпілих, більшістю їх вчинення у молодіжному середовищі, низьким рівнем моралі у суспільстві та правової обізнаності, а також важкістю виявлення правопорушників. Відповідно, більш достовірними є дані UNICEF, згідно яких в Україні близько 50% підлітків були жертвами кібербулінгу [2]. При цьому статистичний аналіз дорослої аудиторії України, яка піддається психологічному цькуванню в мережі Інтернет, відсутній.

Аналіз останніх досліджень і публікацій. Проблеми правового регулювання кібернасильства в Україні, а також особливості його проникнення у соціальне середовище вивчалося такими науковцями як А. Ведернікова, В. Герасимюк, Ю. Градова, В. Гріга, А. Зінцова, Г. Кабенгеле, Н. Когутяк, О. Лапа, І. Лубенець, Л. Найдьонова, Н. Пантєлєєва, М. Фадєєва та іншими. Водночас, вивчення кібернасильства здійснюється у контексті аналізу кіберзлочинності, забезпечення безпеки неповнолітніх у мережі Інтернет.

Виклад основного матеріалу. З поширенням доступу до Інтернету кібернасильство стало одним із самих розповсюджених видів булінгу, отримавши назву кібербулінг або кіберзалякування. Слід відмітити, що у майже всіх наукових джерелах ці поняття визначаються як тотожні. У той же час проблема України проявляється у тому, що у ній нормативного визначення кібернасильства не існує.

Що стосується наукового дослідження даної проблематики, то інтерес до неї постійно посилюється. Зокрема, І. Лубенець визначає кібернасильство як «систематичні умисні дії з боку особи, або групи осіб (частіше підлітків) із використанням інформаційно-комунікаційних засобів, спрямовані проти іншої особи (осіб), що характеризуються створенням ворожої, приниженої обстановки й метою або наслідкам яких є залякування, порушення права на безпечне навчання, повагу, честь, гідність, майно, здоров'я і життя та обмеження свободи волевиявлення особи (осіб) тощо» [3, с. 178]. У свою чергу, Л. Найдьонова під кібербулінгом розуміє новітню форму агресії, що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж тощо [4, с. 2]. А.О. Ведернікова визначає кібербулінг як булінг, що здійснюється із застосуванням засобів електронних комунікацій [5, с. 42]. В.О. Ковтун у своєму визначенні звертає увагу на такі ознаки кібергулінгу як агресія та жорстокість з метою дошкуляння, приниження людини [6, с. 86].

З огляду на наведені визначення вважаємо за можливе вивести окремі ознаки, які є притаманними кібернасильству як явищу: 1) виступає агресивною формою насильства; 2) об'єктом кібербулінгу можуть бути як знайомі, так і незнайомі особи; 3) здійснюється із застосуванням засобів електронних комунікацій; 4) має на меті приниження людини, дошкуляння їй, провокування конфліктних ситуацій.

А.О. Ведернікова також визначає ряд особливостей кібербулінгу, зокрема, це тяжкість встановлення винного, системність дій, неможливість приховатися від протиправних дій та їх наслідків [5, с. 43]. Ми також погоджуємося з авторкою, що встановлення чіткого понятійного апарату дозволяє налагодити протидію цьому виду насильства. Зі свого боку, вважаємо, що визначення поняття кібербулінгу є необхідним на законодавчому рівні.

На жаль, на сьогоднішній день лише один із проявів кібербулінгу отримав мінімальний механізм попередження та припинення на рівні Кодексу України про адміністративні правопорушення. Мається на увазі ст. 173-4 КУпАП «Булінг (цькування) учасника освітнього процесу» [7]. Однак, одразу виникає питання щодо суб'єктного складу даної норми, адже не є зрозумілим, чому потерпілими від даного виду правопорушень законодавець визначає лише учасників освітнього процесу. Оскільки від

кіберцькування на сьогоднішній день можуть потерпати й інші члени суспільства з безліччю соціальних ролей та правових статусів. При цьому необхідність правового регулювання кібербулінгу обумовлюється масштабністю його проявів у суспільстві.

Зокрема, науковцями визначається, що кібернасильство має велику кількість різновидів: використання особистої інформації; анонімні погрози; телефонні дзвінки з мовчанням; переслідування (як елемент фізичного переслідування, шляхом розсилки повідомлень на електронну пошту чи телефон, збирання інформації про жертву, відстеження її переписки); тролінг (розміщення провокаційних повідомлень у мережі); хепі-слепінг (happy slapping) (насильство заради розваги, у тому числі знімання насильства на камеру для подальшого розповсюдження в мережі); сексуальні посягання [5, с. 43].

І. Лубенець виокремлює такі типи поведінки як перепалки (флеймінг), що включає обмін короткими репліками; обмовляння – розповсюдження принизливої інформації; нападки за допомогою образливих повторюваних повідомлень; самозванство, яке реалізується через утілення в певну особу, а точніше жертву з використанням її паролів, акаунтів у соцмережах; відчуження (остракізм); ошуканство через видурювання конфіденційної інформації та її розповсюдження; кіберпереслідування [3, с. 180].

Вважаємо за потрібне звернутися до досвіду зарубіжних країн у цій сфері. Одним із напрямків протидії кібернасильству є його криміналізація. Наприклад, у Курдистані, який є федеративним регіоном Іраку, у 2008 році був прийнятий закон № 6, що криміналізував дифамацію та неналежне використання сучасних засобів зв'язку, якщо воно веде до ганьби чи порушення приватного життя [6]. Вважаємо, що в Україні слід також звернути увагу на віднесення подібних правопорушень до кримінально караних, враховуючи тяжкість наслідків, що настають після вчинення даного правопорушення.

Важливим є досвід Канади, де в основу профілактичної діяльності покладені державні молодіжні програми, спрямовані на попередження насильства та кібернасильства як його складової. Керівниками державних програм по попередженню насильства надаються рекомендації уряду Канади щодо дій, які б впливали на розповсюдження насильства серед жителів країни. Також на рівні уряду ініціюються постійні інклюзивні освітні програми та ініціативи у кампусах навчальних закладів, які стосуються гендерного насильства та примирення. Більше того, у середовищі канадських волонтерів та громадських організацій, спрямованих на захист від кібернасильства, формується теорія «цифрового громадянства», яка передбачає розуміння користувачами соціальних мереж своїх прав на безпечні та інклюзивні онлайн-об'єднання. Зазначені «цифрові громадяни» можуть діяти як реалізатори онлайн-проекту «Neighborhood Watch», сигналізуючи соціальним мережам у разі використання їх платформ для здійснення актів насильства чи жорстокого поводження [7]. Зауважимо, що досвід залучення до попередження кібербулінгу громадян не є новим. Зокрема, поліція Нідерландів розробила програму щодо залучення засуджених молодих хакерів до легальної роботи у пілотному проекті Hack_Right. Ця програма спрямована на протидію кіберзлочинності та заохочення до «етичного злому» на заміну кримінальному покаранню [8].

Окремою проблемою для належного реагування правоохоронних органів на кібернасильство є відсутність розподілу повноважень між Національною поліцією України та Департаментом кіберполіції Національної поліції України щодо протидії кібернасильству. Враховуючи, що кібернасильство не визначається у діючому законодавстві як кримінальне правопорушення, то можна передбачити, що воно не підпадає під юрисдикцію кіберполіції, яка відповідно до Положення про Департамент кіберполіції Національної поліції України забезпечує протидію кримінальним правопорушенням у кіберсфері. Однак, слід відмітити, що під час звернень громадян до Національної поліції з'ясовується, що у Національній поліції немає відповідного матеріально-технічного забезпечення та навичок розкриття і розслідування даних видів правопорушень. У якості при-

кладу безпорадності у цьому питанні правоохоронних органів можна привести спробу медіаекспертки та тренерки з безпеки для журналістів Інституту масової інформації Ірини Земляної покарати осіб, які здійснювали масовий кібербулінг на її сторінці у соцмережі Facebook. На її звернення до кіберполіції (при наявності самостійно зібраних доказів) їй порадили звернутися до поліції, а у поліції – звернутися до кіберполіції. Бо, як зазначили посадовці з обох сторін, це питання не відноситься до їх компетенції [2].

У даному випадку впадає в око незаконність відмови правоохоронних органів у захисті охоронюваних законом прав. Пункт 3 ст. 2 Закону України «Про основні засади забезпечення кібербезпеки України» дійсно встановлює, що дія даного закону, як основа діяльності кіберполіції, не розповсюджується на «соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси)» [11]. Однак, у Законі є зауваження - «якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів» [11]. У даному випадку виникає питання, чи не є приватна інформація, честь, гідність особи такою, що повинна охоронятися законом? Однозначно так! При цьому ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» встановлює об'єктами кібербезпеки в першу чергу конституційні права і свободи людини і громадянина. І в даному та схожому випадках проблема полягає у тому, що відсутній чіткий нормативно визначений механізм, який би на належному рівні забезпечував захист особи від кібернасильства. І в цій позиції ми спільні з багатьма науковцями. Зокрема, А.О. Ведерникова пропонує забезпечення кримінально-правового регулювання кібернасильства, оскільки відсутність подібної норми «зв'язує руки» правоохоронним органам.

Окрім зазначеного, Україні слід дослухатися до позиції ООН, яка проявляється через вимогу ратифікації Стамбульської конвенції Ради Європи, що повинно стати іще одним кроком до подолання насильства в українському суспільстві. При цьому, вважаємо, що одні релігійні, політичні чи моральні позиції, які висловлюються наразі в українському суспільстві не варті уваги на шляху до формування належного механізму захисту людського життя та здоров'я.

Важливим кроком до розуміння сутності кібербулінгу та напрямків протидії йому завжди виступає юридична практика, зокрема практика судів. На сьогоднішній день існує низка рішень Європейського суду з прав людини, які стосуються порушення прав особи у соціальних мережах. Зокрема, справа K.U. v. FINLAND (Application no. 2872/02) [12] стосується потерпілого, відносно якого невідомі особи, коли йому виповнилося 12 років, розмістили інформацію на веб-сайті знайомств без його відома. Інформація містила його вік та рік народження, детальний опис його фізичного розвитку, фотографію, а також номер телефону, який відрізнявся від дійсного лише однією цифрою. При цьому в інформації стверджувалося, що він шукає інтимних стосунків із хлопчиками його віку чи старше. Батько заявника звернувся до поліції з проханням встановлення особи, однак постачальником інтернет-послуг у даній інформації було відмовлено через конфіденційність такої інформації. При цьому навіть звернення до органів поліції та подальше звернення до суду з метою покарання постачальника інтернет-послуг та отримання інформації не дало результатів через те, що дії зловмисника насправді не містили ознак кримінального правопорушення, передбаченого законодавством, а саме зловмисне викривлення інформації. Апеляційний суд та Верховний суд відмовили у задоволенні апеляції. ЄСПЛ відзначив, що факти, які лежать в основі публікації на веб-сайті, стосуються приватного життя, яке охоплює фізичну та моральну цілісність особи і вимагає при розгляді подібних справ брати до уваги потенційну загрозу фізичному та психічному добробуту заявника з огляду на його вразливість через молодий вік. При цьому суд наголошує, що у подібних випадках зобов'язання держави по охороні приватного життя особи дозволяють державі втручатися у міжособистісні відносини, що залежить від конкретного аспекту приватного

життя. У той же час Суд приходить до висновку, що стримування окремих вчинків вимагає від держав ефективних кримінально-правових норм.

Вважаємо, що означена позиція Європейського суду з прав людини є важливою підставою для перегляду національної політики щодо протидії насильству як соціального явища взагалі, так і кібернасильства зокрема.

Висновки. Таким чином, слід зазначити, що подолання кібернасильства в Україні, у тому числі силами Національної поліції, потребує комплексних заходів з боку правоохоронних органів та судових організацій, а також української держави. На наш погляд, це стосується створення належного механізму правового регулювання з протидії кібернасильству, який чітко визначатиме правовий статус та юрисдикцію органів досудового та судового провадження, які забезпечують протидією кібернасильству. Окрім цього означені механізми мають регламентувати порядок звернення і захисту жертв кібербулінгу до правоохоронних органів. У цьому напрямку також важливим аспектом виступає створення інституту кримінальної відповідальності за кібернасильство. Окрім цього, актуальну роль у протидії кібернасильству відіграє розробка відповідних державних програм протидії кібербулінгу та підтримка з боку держави громадських ініціатив та дій громадських організацій у цій сфері.

Література

1. В Україні презентували перше комплексне дослідження про кібербулінг. URL: https://thedigital.gov.ua/news/ (дата звернення 22.02.2021).

2. Чернова О. Кібербулінг – це легко, просто коментуєш і ховаєшся: історії про цькування в інтернеті. URL: https://hromadske.ua/posts/ (дата звернення 22.02.2021).

3. Лубенець І. Кібернасильство (кібербулінг) серед учнів загальноосвітніх навчальних закладів. *Jurnalul Juridi National: teore si practica*. Junie, 2016. С. 178-182.

4. Найдьонова Л.А. Кібербулінг або агресія в Інтернеті: способи розпізнання і захист дитини: методичні рекомендації. Вип. 4. Київ, 2011. 34 с.

5. Ведернікова А.О. Необхідність кримінально-правового регулювання кібербулінгу. *Протидія кіберзагрозам та торгівлі людьми* (26 лист. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2019. С. 42-46.

6. Ковтун В.О. Протидія кібербулінгу як сучасній формі агресії *Протидія кіберзагрозам та торгівлі людьми* (26 лист. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2019. С. 86-88.

7. Кодекс України про адміністративні правопорушення: Закон України від 07 груд. 1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення 22.02.2021).

8. COVID-19, gender and cyber violence in the kurdistan region. URL: https://www.sciencespo.fr/ceri/en/content/covid-19-gender-and-cyber-violence-kurdistan-region (дата звернення 22.02.2021).

9. Taking action to end violence against young women and girls in Canada. URL: https://www.ourcommons.ca/DocumentViewer/en/42-1/FEWO/report-7/page-54 (дата звернення 22.02.2021).

10. Stephen Pritchard. Hack_Right: Dutch cybercrime prevention program comes of age. The Daily Swig: Cybersecurity news and views. 14 August 2020. URL: https://portswigger.net/daily-swig/hack-right-dutch-cybercrime-prevention-program-comes-of-age (дата звернення 22.02.2021).

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.03.2021).

12. K.U. v. FINLAND (Application no. 2872/02). URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]} (дата звернення 11.03.2021).

References

1. V Ukraini prezentuvaly pershe kompleksne doslidzhennia pro kiberbulinh. URL:

https://thedigital.gov.ua/news/ (data zvernennia 22.02.2021).

2. Chernova O. Kiberbulinh – tse lehko, prosto komentuiesh i khovaieshsia: istorii pro tskuvannia v interneti. URL: https://hromadske.ua/posts/ (data zvernennia 22.02.2021).

3. Lubenets I. Kibernasylstvo (kiberbulinh) sered uchniv zahalnoosvitnikh navchalnykh zakladiv. *Jurnalul Juridi National: teore si practica*. Junie, 2016. S. 178-182.

4. Naidonova L.A. Kiberbulinh abo ahresiia v Interneti: sposoby rozpiznannia i zakhyst dytyny: metodychni rekomendatsii. Vyp. 4. Kyiv, 2011. 34 s.

5. Vedernikova A.O. Neobkhidnist kryminalno-pravovoho rehuliuvannia kiberbulinhu. Protydiia kiberzahrozam ta torhivli liudmy (26 lyst. 2019 r., m. Kharkiv) / MVS Ukrainy, Kharkiv. nats. un-t vnutr. sprav; Koordynator proektiv OBSIe v Ukraini. Kharkiv: KhNUVS, 2019. S. 42-46.

6. Kovtun V.O. Protydiia kiberbulinhu yak suchasnii formi ahresii Protydiia kiberzahrozam ta torhivli liudmy (26 lyst. 2019 r., m. Kharkiv) / MVS Ukrainy, Kharkiv. nats. un-t vnutr. sprav; Koordynator proektiv OBSIe v Ukraini. Kharkiv: KhNUVS, 2019. S. 86-88.

7. Kodeks Ukrainy pro administratyvni pravoporushennia: Zakon Ukrainy vid 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/ laws/ show/80731-10#Text (data zvernennia 22.02.2021).

8. COVID-19, gender and cyber violence in the kurdistan region. URL: https://www.sciencespo.fr/ceri/en/content/covid-19-gender-and-cyber-violence-kurdistan-region (data zvernennia 22.02.2021).

9. Taking action to end violence against young women and girls in Canada. URL: https://www.ourcommons.ca/DocumentViewer/en/42-1/FEWO/report-7/page-54 (data zvernennia 22.02.2021).

10. Stephen Pritchard. Hack_Right: Dutch cybercrime prevention program comes of age. The Daily Swig: Cybersecurity news and views. 14 August 2020. URL: https://portswigger.net/daily-swig/hack-right-dutch-cybercrime-prevention-program-comes-of-age (data zvernennia 22.02.2021).

11. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia 11.03.2021).

12. K.U. v. FINLAND (Application no. 2872/02). URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]} (data zvernennia 11.03.2021).

M. Novikov, M. Novikova

THEORETICAL AND LEGAL ASPECT OF CYBER VIOLENCE: NOTION AND CONTENT

Kherson Faculty of Odesa State University of Internal Affairs
Fonvizin str., 1, 73000, Kherson, Ukraine,
E-mail: novikovamariia1222@gmail.com

*The **purpose** of the theses is to analyze some aspects of the cyber violence, which has theoretical, legal and applied character. The main tools of such violence are finding and using computer technics, cybernetic (general and local) computer net by a circle of persons during a certain period of time, in some space and inflicting other people psychically, biologically, physically, economically, financially; property and weapons are involved as well. **The methods of research** are general scientific and special methods of scientific cognition, including the dialectical method, methods of formal logic, structural-logical method, categorical, etc. **Results:** it is determined that overcoming cyber violence in Ukraine requires the formation of a system of comprehensive measures. First of all, it concerns the creation of an appropriate mechanism of legal regulation, which will clearly define the legal status of bodies and units that will deal with the issue of combating cyberbullying. **Discussion:** the cyber violence is known to suppress its victims' consciousness and will by those people having an active motivation and socially dangerous or deviant behavior. Such behavior destabilizes the society and state as well and general human values (a human being with his or her rights and freedoms; a modern state and law; civil society and democracy; mechanisms of state power regarding its centralization and decentralization with the division of the latter into tree branches etc) are getting ruined.*

The most of cyber violence cases are known to take place among young people with the low level of social morality and culture and legal knowledge as well. In such a society, it is difficult to find offenders mocking those who are weaker than they. According to the more true data of the UNICEF, 50% of teenagers in Ukraine were victims of such violence. The statistical analysis of the cyber violence among the Ukrainian adults is unknown or latent because the form of psychological persecution is hidden in the mobile nets like Instagram, Telegram etc.

Keywords: *cyber violence; cyber crime; objects; subjects; cyber violence content; international cyber violence; state and suprastate cyber violence; intented and unintended cyber violence.*