

Список використаних джерел:

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. 2015. № 40-41. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>.

2. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

3. Наказ МВС України від 03.08.2017 № 676 (zareєстровано в Міністерстві юстиції України 28 серпня 2017 р. за № 1059/30927) «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»». URL: <https://zakon.rada.gov.ua/laws/show/z1059-17#Text>.

***Бехтер Ростислав Олександрович**
курсант 206 навчальної групи ННІ № 3
НАВС, рядовий поліції*

*Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший
викладач кафедри інформаційних
технологій та кібербезпеки ННІ № 1
НАВС, капітан поліції*

АНАЛІЗ ПРОБЛЕМ КІБЕРБУЛІНГУ ТА ОНЛАЙН-ПЕРЕСЛІДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

У зв'язку з воєнним станом, проблема кібербулінгу та онлайн-переслідування набуває особливого значення. Це важливе явище, яке може поглибити соціальні та психологічні напруження в суспільстві та серед військовослужбовців. Кібербулінг, як і офлайн булінг, може призвести до серйозних наслідків для жертв, зокрема до стресу, депресії та інших психічних проблем. Онлайн-переслідування може стати інструментом для дестабілізації та дискредитації ворожих сил. На передовій це може викликати додаткові труднощі для військових, зокрема збільшити їх вразливість та відволікання від виконання бойових завдань. Для вирішення цих проблем необхідно розробити комплексні стратегії кібербезпеки, включаючи навчання персоналу, використання захисту даних та моніторингу соціальних мереж. Такі заходи допоможуть зменшити вплив кіберагресії на військовий контекст та забезпечити безпеку та захист учасників конфлікту.

Проблематика кібербулінгу та засоби протидії йому представляють новий напрямок для наукового дослідження на сьогодні, оскільки поки що не проводилися глибокі наукові дослідження з цієї теми.

Деякі вчені лише дотепер звертали увагу на окремі аспекти кібербулінгу, тоді як інші аналізували лише проблематику булінгу та кібербезпеки. Роботи відомих дослідників, таких як С. Албул, Р. Гришук, М. Грінченко, С. Гнятюк, І. Діордіц, Л. Лушпай, Д. Лейн, О. Ожйова, В. Петросянець, С. Стельмах, А. Губко, Ю. Савальєв, О. Ліщинська, Н. Новікова, О. Корченко, В. Ліпкан, С. Мельник, В. Кашук, І. Катеренчук, В. Грохольський, П. Біленчук, І. Севкова та інших, включають аналізи цих тем, але дотепер не було проведено комплексного наукового дослідження.

Термін «кібербулінг» походить від двох англійських слів: «кібер» і «булінг». «Кібер» означає віртуальне комп'ютерне середовище; «Bull» означає бик, бугай, галаслива людина, в переносному значенні – дуже сильна агресивна людина.

Офіційний веб-сайт UNICEF надає таке визначення поняття кібербулінгу, а також приводить приклади цього явища:

- поширення брехні про когось або розміщення фотографій, які компрометують когось, у соціальних мережах;
- надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями;
- видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені [1].

Як вказує В.М. Фурашев, кібербулінг – це новітня форма агресії, яка передбачає собою напади з метою завдання психологічної шкоди: насміхання, цькування, маніпулювання через інформаційно-комунікаційні засоби, а саме: мобільний телефон, електронну пошту, соціальні мережі й ін. [2, с. 73].

На нашу думку, кібербулінг або кібермоббінг, представляє собою сучасну форму агресії, яка включає в себе заподіяння страждань дітям один одному, а також жорстокі дії від дорослих, що здійснюються в Інтернеті за допомогою мобільних телефонів, комп'ютерів, електронної пошти, соціальних мереж тощо.

У сучасному віртуальному світі розповсюджені форми кібербулінгу, такі як анонімні загрози, надіслані телефонні дзвінки, тролінг, стеження, сексуальні домагання, флеймінг, розповсюдження обмов, шахрайство, кіберпереслідування та інші види насильства.

У цьому контексті слід відзначити, що механізм адміністративно-правового регулювання кібернетичної та інформаційної сфери спрямований на захист як національних інтересів, так і інтересів окремих осіб. Адміністративно-правові принципи виконують різноманітні функції, як загальні, так і спеціалізовані, щоб визначити основні заходи та засоби протидії різним негативним кіберзагрозам та кібератакам [3, с. 202].

Тобто встановлення адміністративно-правових засад кібербулінгу – це процес регулювання явища кібербулінгу та визначення заходів його протидії на цій основі. Аналіз існуючого законодавства України показує відсутність чіткого визначення кібербулінгу, що вимагає покращення.

Однак, оскільки кібербулінг є формою кіберзагроз, можна стверджувати, що адміністративні засади забезпечення кібернетичної та інформаційної безпеки в Україні в певній мірі охоплюють регулювання кібербулінгу, але потребують законодавчих корективів.

Тому вважаємо, що для ефективного створення адміністративно-правової бази протидії кібербулінгу, важливо розуміти сутність поняття «адміністративно-правові засади». Зазначене включає в себе систему юридичних норм, що визначають суть, принципи, завдання, форми та види кібербулінгу.

У підсумку, ефективне розв'язання проблеми кібербулінгу потребує комплексного підходу, який базується на створенні та впровадженні відповідних адміністративно-правових засад. Ці засади мають включати чітко визначення термінів, принципів, завдань та форм кібербулінгу, а також ефективні механізми для його протидії. Важливо постійно оновлювати та вдосконалювати законодавство з питань кібербезпеки, а також проводити освітню та інформаційну роботу серед населення, зокрема серед молоді, щоб підвищити усвідомлення щодо наслідків кібербулінгу та методів його запобігання. Тільки взаємодія громадських організацій, урядових структур, освітніх закладів та інших зацікавлених сторін може призвести до зменшення випадків кібербулінгу та створення безпечного середовища в Інтернеті для всіх користувачів.

Список використаних джерел:

1. Кібербулінг: матеріал з офіційного сайту ЮНІСЕФ. URL: <https://www.unicef.org/ukraine/cyberbullying> (дата звернення: 09.04.2024).

2. Фурашев В. М. Інформаційна небезпека: Кібербулінг. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали міжнар. наук.-практ. конф. (м. Київ, 21 квіт. 2017 р.). Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»; вид-во «Політехніка». 2017. Ч. II. С. 72–75.

3. Чумак В. В., Цебинога В. Ю. Правове регулювання протидії кібербулінгу в Україні. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали міжнародної наук.-практ. конф. (м. Харків, 30.11.2018 р.) (МВС України, Харків. нац. ун-т внутр. справ; Консультат. місія Європейського Союзу). Харків, 2018. С. 202–204.