4. Synchron.ua. Кібератаки на бізнес України 2025: Нові Вектори Загроз та Виклики. 2025.

5. Detector Media. Верховна Рада ухвалила закон про кіберзахист державних ресурсів. 2025.

6. LSEJ (Legal Studies and Economic Journal). Роль технологій штучного інтелекту у правоохоронній діяльності. 2024.

7. BDO Україна. Роль штучного інтелекту в кібербезпеці: передбачення і запобігання атак. 2025.

8. Visnyk Juris (Журнал юридичних досліджень). Зарубіжний досвід використання штучного інтелекту для протидії кіберзлочинам. 2025.

9. LIGA360. Державне регулювання штучного інтелекту в Україні. 2025.

10. НАВС (Національна академія внутрішніх справ України). Міжнародний досвід правового регулювання небезпеки ШІ. 2025.

11. Держателеві дослідження та аналітика українського ринку кібербезпеки 2017-2025 років, MS Detector.

Радіонова Валерія Іванівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРБУЛІНГ І ПЕРЕСЛІДУВАННЯ В МЕРЕЖІ: ПРОГАЛИНИ ЗАКОНОДАВСТВА

У цифрову епоху Інтернет перетворився не лише на зручний засіб спілкування, але й на простір, де все частіше фіксуються випадки психологічного насильства, зокрема

кібербулінг і кіберсталкінг. Ці явища порушують право кожного на невтручання в особисте і сімейне життя, закріплене статтею 32 Конституції України право кожного на невтручання в особисте і сімейне життя [1], а також статтю 17 Міжнародного пакту про громадянські і політичні права, згідно з якою «ніхто не може зазнавати свавільного або незаконного втручання в його особисте життя, недоторканність житла чи кореспонденції, або посягань на його честь і репутацію» [2].

Мета роботи полягає у всебічний аналіз проблеми кримінальної відповідальності за кібербулінг і переслідування в мережі в Україні. Основне завдання – виявити прогалини чинного законодавства та окреслити шляхи його вдосконалення з урахуванням міжнародних стандартів захисту прав людини.

Кібербулінг – це навмисне, повторюване та систематичне здійснення протиправних дій, що мають нав'язливий характер і спрямовані на приниження, переслідування або створення психологічного тиску на людину. Це може проявлятися у формі цькування, залякування чи приниження через засоби електронної комунікації. В Україні це явище частково регулюється положеннями Кодексу України про адміністративні правопорушення [3], проте запроваджені заходи відповідальності недостатньо враховують серйозні наслідки, які можуть негативно впливати на психологічний стан постраждалих.

Доктор юридичних наук О. Бандурка вказує на те, що адміністративна відповідальність за кібербулінг не відповідає рівню суспільної небезпеки цього правопорушення, оскільки воно часто перебуває на межі з кримінально караними формами насильства [4].

Відсутність законодавчого визначення терміну «кіберсталкінг» створює значні прогалини у формулюванні та регламентації цього поняття в контексті чинного законодавства України. На основі проведеного аналізу можна припустити, що поняття «кібербулінг» може бути тлумачено як переслідування особи з використанням засобів Інтернету, соціальних мереж або месенджерів.

Подібні дії можуть потрапляти під регулювання статті 126-1 Кримінального кодексу України, яка охоплює випадки домашнього насильства, статті 182, що передбачає відповідальність за порушення права на недоторканність приватного життя, статті 129, яка стосується погрози вбивством,

а також статті 153, що установлює відповідальність за сексуальне насильство Кримінального кодексу України [5].

Відсутність конкретного визначення призводить до зволікання з розслідуванням і безкарності переслідувачів, адже, правова кваліфікація кіберсталкінгу в Україні ускладнена саме через невизначеність складу злочину, що унеможливлює диференціацію між жартом, переслідуванням та психологічним насильством [6].

Ратифікація Україною Стамбульської конвенції (далі – Конвенція) [7] відкрила шлях до криміналізації зазначених вище дій. Стаття 34 Конвенції прямо зобов'язує держави-учасниці вжити необхідних законодавчих або інших заходів для криміналізації навмисного переслідування, що викликає у потерпілої особи страх за свою безпеку. У рекомендаціях Групи експертів Ради Європи з протидії насильству (GREVIO) наголошується, що переслідування у цифровому середовищі становить ту саму загрозу, що і фізичне наближення, тому має отримати однакову правову оцінку [8].

Практика Європейського суду з прав людини підтверджує, що держава несе позитивні зобов'язання щодо захисту осіб від кіберпереслідування. У справі Buturuga v. Romania (2020), Суд постановив, що відсутність належної реакції органів влади на переслідування в мережі є порушенням статей 3 і 8 Конвенції про захист прав людини і основоположних свобод. де ЄСПЛ визнав, що «кіберпереслідування, як і фізичне, становить форму насильства, яка має бути ефективно розслідувана державою» [9].

Питання, порушене в цій роботі, є досить новим для українського правового поля. У зв'язку із глобалізацією суспільства та стрімким розвитком Інтернет-середовища, законодавству, яке створювалося понад 15 років тому, стає дедалі складніше адаптуватися до сучасних реалій. Наразі українське законодавство демонструє свою недосконаліть через низку прогалин, зумовлених динамічними змінами цифрового середовища. До найбільших проблем можна віднести:

1. Відсутність чіткого законодавчого визначення терміна «кіберсталкінг».

2. Правове регулювання кібербулінгу обмежується лише адміністративною відповідальністю, без урахування можливостей кримінального переслідування.

3. Недостатня розробка єдиної методики розслідування таких злочинів.

4. Невизначеність і недостатня сформованість судової практики у цій сфері.

Сучасне кримінальне право має бути адаптоване до цифрових реалій, адже поява нових способів вчинення злочинів потребує впровадження відповідних механізмів їх протидії [10].

Для вирішення зазначених проблем необхідно:

1. Прийняти спеціальний закон про протидію кібернасильству.

2. Внести зміни до Кримінального кодексу України, передбачивши окремий склад злочину під назвою «переслідування в цифровому просторі».

3. Розробити і впровадити національні програми, спрямовані на підвищення цифрової грамотності та безпеки.

4. Створити ефективну систему психологічної підтримки жертв кібернасильства.

5. Підготувати правоохоронців до роботи з електронними доказами та забезпечити їх належними інструментами для боротьби з такими правопорушеннями.

Україна потребує сучасного підходу до цих викликів, аби забезпечити ефективний захист прав громадян у новітньому цифровому середовищі.

Висновок. Кібербулінг є новою формою насильства, яка порушує базові права людини на гідність, безпеку та приватність. В Україні відсутнє конкретне кримінально-правове визначення таких дій, що значно ускладнює притягнення винних до відповідальності. З урахуванням міжнародних стандартів, зокрема вимог Стамбульської конвенції та практики Європейського суду з прав людини, виникає необхідність запровадження в Кримінальному кодексі України окремих статей, які б визначали відповідальність за переслідування та цькування в цифровому просторі. Такий крок сприятиме реальному захисту постраждалих і стане важливим етапом у створенні безпечного правового простору в Інтернеті.

Список використаних джерел

1. Конституція України від 28.06.1996 р.

2. Міжнародний пакт про громадянські і політичні права від 16.12.1966р.

3. Закон України «Про ратифікацію Конвенції Ради Європи про запобігання насильству щодо жінок і домашньому насильству та боротьбу з цими явищами» № 2319-IX від 20.06.2022 р.

4. Кодекс України про адміністративні правопорушення.

5. Бандурка О. М. Цифрова безпека особи у контексті кримінального права України. Харків : Право, 2021.

6. Кримінальний кодекс України.

7. Стамбульської конвенції Закон № 2319-IX від 20 червня 2022 р.

8. GREVIO. Baseline Evaluation Report on Ukraine (2023). Council of Europe.

9. Постанова ЄСПЛ у справі Buturuga v. Romania (Application no. 56867/15), 11 лютого 2020 р.

10. Тацій В. Я. Кримінальне право України: проблеми адаптації до європейських стандартів. Харків: Право, 2022.

Романська Валерія Ігорівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Семенов В. В., доцент кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ОПТИМІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

У сучасному світі стрімкий розвиток інноваційних розробок зумовлює появу новітніх векторів вдосконалення у всіх сферах життєдіяльності: медицині, промисловості, фінансах та, що особливо важливо, у правоохоронній діяльності та криміналістиці. З кожним днем інформаційні технології стають невід'ємною частиною нашого повсякденного життя, відіграючи ключову роль у вирішенні складних завдань та оптимізації різноманітних процесів.