5. Про розвідку : Закон України від 17 вересня 2020 р. № 912–IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/912IX#Text

6. Про Національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/main/56/2022.#Text

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19.03.2022 № 152/2022. URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text

Сердечна Анастасія Романівна,
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

КЛАСИФІКАЦІЯ ТА ТИПОЛОГІЧНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ ОСОБИ ПОТЕРПІЛОГО В КІБЕРПРОСТОРІ

Станом на початок 2025 року в Україні інтернетом користувався 31,5 млн людей, а рівень проникнення доступу до мережі склав 82,4 %. Для порівняння зазначимо, що в Східній Європі цей показник складає 90,6 %. З січня 2024 року до січня

2025 року кількість інтернет-користувачів в Україні зросла на 690 000 (або на 2,2 %) [1]. Стрімка діджиталізація суспільства створила появу нових форм кримінальних посягань, серед яких особливе місце посідають кібербулінг [2], кібершахрайство та кіберсталкінг. Незважаючи на схожість у механізмах впливу на особу, кожна із наведених форм злочинної поведінки характеризується власними траєкторіями віктимності, які визначають особливості реакцій жертв, рівень ризику та способи протидії. Вивчення поведінкових моделей потерпілих та їх соціально-психологічних характеристик є важливим для розробки ефективних механізмів профілактики та підтримки.

Мета цієї публікації полягає у визначенні науково обґрунтованих підходів до класифікації та типологізації особи потерпілого у кіберпросторі, виявленні основних критеріїв її диференціації залежно від характеру кіберзагроз, рівня цифрової компетентності, соціально-психологічних особливостей та поведінкових стратегій, а також формулюванні типологічної моделі, що сприятиме глибшому розумінню механізмів віктимізації в умовах цифрового середовища.

Віктимність у кіберпросторі розглядається як комплексна соціально-психологічна категорія, що характеризує особу як потенційну або фактичну жертву правопорушення. У наукових публікаціях підкреслюється, що її детермінантами є вік, соціально-економічний статус, рівень цифрової грамотності, ступінь відкритості персональних даних у мережі та психологічні особливості особи .

Науково-методологічно обґрунтована класифікація має спиратись на такі основні принципи як:

1. Мультидименсійність – поєднання технічного, соціально-психологічного і правового вимірів віктимізації.

2. Практична орієнтованість – виділення типів, що потребують різних форм захисту та реагування (технічна допомога, психологічна підтримка, кримінально-правовий захист).

3. Динамізм – визнання змінності статусу особи (наприклад, постраждалий може стати суб’єктом ризикованої поведінки або контрагентом у ланцюгу інциденту).

Саме на основі цих принципів, комплексних критеріїв класифікації різних типів кіберзагроз [3] та досліджень [4] формується науково обґрунтована класифікація потерпілих у

кіберпросторі, що дозволяє виділити типові групи постраждалих, визначити закономірності їх віктимності та розробити диференційовані заходи превенції, захисту та реабілітації. Таким чином, подальший розгляд буде зосереджено на описі основних підходів до класифікації та типології потерпілих у цифровому середовищі.

1. За характером взаємодії з правопорушником. Безпосередні потерпілі – особи, проти яких здійснено цілеспрямоване втручання (наприклад, фішинг, хакерська атака, вимагання). Опосередковані потерпілі – користувачі, що зазнали шкоди внаслідок масових атак або витоку даних, без прямого контакту з правопорушником.

2. За рівнем цифрової компетентності. Технічно необізнані особи, що стають жертвами кібершахрайства або соціальної інженерії. Користувачі із середнім рівнем знань, які не дотримуються основ кібергігієни. Професійні користувачі та адміністратори, що зазнають високотехнологічних атак.

3. За соціально-психологічними ознаками. Вразливі категорії (діти, підлітки, літні люди, особи з низьким рівнем критичного мислення) – часті жертви кібербулінгу, маніпуляцій чи секстингу. Соціально активні користувачі, які свідомо ризикують, публікуючи надлишкову кількість персональної інформації.

4. За видом шкоди, якої завдано. Матеріальна (економічна) – незаконне заволодіння коштами або майном через електронні засоби. Інформаційна – витік персональних чи конфіденційних даних. Психологічна – кібербулінг, кіберсталкінг, онлайн-насильство. Репутаційна – поширення компрометуючої інформації, підробка профілю.

5. За суб'єктним статусом. Фізичні особи – індивідуальні користувачі, які потерпають від персоналізованих атак [5]. Юридичні особи – організації, що зазнали втручання у діяльність їхніх інформаційних систем (наприклад, злам баз даних, атакування сайтів) [6].

На основі зазначених критеріїв можна виокремити кілька типологічних груп:

1. Технічно вразливі користувачі, які не володіють достатніми знаннями щодо цифрової безпеки.

2. Психологічно вразливі особи, схильні до довірливості чи емоційних реакцій, що використовуються правопорушниками.

3. Ризиковані користувачі, які свідомо нехтують правилами безпеки, публікують персональні дані або беруть участь у сумнівних онлайн-активностях.

4. Інституційні потерпілі, для яких шкода має економічний або репутаційний вимір (державні установи, банки, освітні організації).

Попри різну природу та мотиви кіберзлочинів їхні траєкторії віктимності мають спільні характеристики, зокрема емоційний стрес, соціальну ізоляцію та психологічну травму. Водночас кожний тип кіберзлочинності формує специфічні наслідки: кібербулінг – переважно психологічні, шахрайство – економічні, кіберсталкінг – комплексні психологічні та соціальні. Це дозволяє розробляти ефективні превентивні заходи, підвищувати рівень цифрової грамотності та вдосконалювати практику взаємодії громадян із правоохоронними органами.

Отже, класифікація потерпілих у кіберпросторі є необхідною умовою для формування цілісного уявлення про механізми віктимізації у цифровому середовищі. А аналіз віктимності у випадках кіберзлочинів, у свою чергу, свідчить, що різні форми кіберзлочинності визначають специфічні траєкторії впливу на жертв, що вимагає комплексного підходу до протидії. Законодавство України, кримінально-правові норми та практика кіберполіції створюють правові рамки для реагування на ці явища, але їх ефективність залежить від поєднання правового регулювання, освіти населення та психологічної підтримки постраждалих. Подальші наукові дослідження мають інтегрувати кримінологічний, психологічний та соціологічний аспекти віктимності у цифровому середовищі для розробки комплексної моделі захисту громадян.

Список використаних джерел

1. Інтернет, соцмережі, стримінги та відео. Найцікавіше зі звіту DIGITAL 2025 про взаємодію з цифровими технологіями. URL: https://mediamaker.me/najczikavishe-zi-zvitu-digital-2025-pro-vzayemodiyu-z-czyfrovymy-tehnologiyamy-16257/

2. Кібербулінг – що це та як це зупинити. 10 фактів, які підлітки хочуть знати про кібербулінг. URL: https://www.unicef.org/ukraine/cyberbulling

3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. [Видання друге, перероб. та доп.]. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.

4. Звіт про кінцеве дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки: підготовлено для Представництва Фонду цивільних досліджень та розвитку США в Україні. URL: info_sapiens_crdf_report_ua_2024.pdf

5. Фінансова допомога від організацій: як не стати жертвою онлайн-шахрайства. URL: https://fakty.com.ua/ua/videos/finansova-dopomoga-vid-organizaczij-yak-ne-staty-zhertvoyu-onlajn-shahrajstva/

6. Мелехова М. Хакери атакують держоргани та ОПК України за допомогою фейкових судових повісток. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20250805-hakery-atakuyut-derzhorgany-ta-opk-ukrayiny-za-dopomogoyu-fejkovyh-sudovyh-povistok/

Старовойт Аліна Олексіївна,
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

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах розвитку цифрових технологій проблема правового регулювання інформаційної безпеки набуває особливої актуальності. Цифровізація державного управління, бізнесу та освіти, а також активне впровадження штучного інтелекту й автоматизованих систем створюють нові ризики для захисту персональних даних, державних інформаційних ресурсів і прав громадян [2, с. 4–5].

Інформаційна безпека – це стан захищеності інформації, інформаційних систем і ресурсів, який забезпечує їхню цілісність, доступність та конфіденційність. В Україні основою правового регулювання у цій сфері є Конституція України, яка