

КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.9

DOI <https://doi.org/10.32838/TNU-2707-0581/2022.2/05>

Бугера О.І.

Національний транспортний університет

СОЦІАЛЬНІ ІНТЕРНЕТ-МЕРЕЖІ ТА ПРОБЛЕМИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У статті досліджено проблеми використання соціальних Інтернет-мереж для запобігання злочинності в сучасних умовах розвитку інформаційно-комунікаційних технологій. Встановлено, що вирішення проблем запобігання злочинності в умовах постійного розвитку інформаційно-комунікаційних технологій потребує проведення відповідних наукових досліджень та загалом переосмислення криминологічних підходів у цій сфері. Наголошено на потенційній небезпеці використання соціальних Інтернет-мереж зі злочинною метою, зокрема, щодо: вчинення кіберзлочинів; збору коштів терористичними угрупованнями для фінансування та пропаганди тероризму, залучення нових членів терористичних організацій; кібербулінгу; розповсюдження дитячої порнографії; поширення (насамперед, серед неповнолітніх) інформації про так звані «групи смерті» тощо. Сформовано напрями використання можливостей соціальних Інтернет-мереж для запобігання злочинності, це зокрема: здійснення моніторингу та аналізу криминологічно значимої інформації для прогнозування злочинності; розроблення та впровадження запобіжних заходів на загальносоціальному, спеціально-криминологічному та індивідуальному рівнях; підвищення рівня комунікації між поліцією і громадянами щодо вирішення проблем запобігання злочинності; використання соціальних Інтернет-мереж для поширення оперативної інформації, щодо розшуку злочинців, повідомлень про вчинені кримінальні правопорушення та можливої небезпеки для мешканців певних територій; інформаційної підтримки в соціальних Інтернет-мережах об'єднань громадян, що визначають пріоритетом в своїй діяльності запобігання злочинності безпосередньо в місцях свого проживання (сусідський нагляд) та ін. Важливим є також розроблення інтерактивного блогу запобігання злочинності з метою налагодження в соціальних Інтернет-мережах комунікаційного зв'язку між працівниками правоохоронних органів (дільничними офіцерами поліції) та мешканцями певних визначених територій щодо обговорення та вирішення проблем запобігання злочинності на локальному рівні (селище, мікрорайон).

Ключові слова: мережа Інтернет, соціальні Інтернет-мережі, інформаційні технології, злочинність, запобігання.

Постановка проблеми. У сучасних умовах розвитку інформаційних технологій та побудови інформаційного суспільства, взаємодія користувачів соціальних Інтернет-мереж, стає не лише засобом комунікації, а й новою сферою життєдіяльності. Користувачі активно та всебічно взаємодіють між собою, що призводить до накопичення великої кількості інформації, яка може мати, у тому числі, й неправомірний характер. Поява та широке поширення у вітчизняному інформаційному просторі соціальних Інтернет-мереж призвела до того,

що організовані злочинні групи й окремі особи, які вчиняють протиправні діяння, стали активно використовувати широкі можливості всесвітньої мережі [1, с. 142]. Як показує світовий досвід, можливості інформаційних технологій та загалом мережі Інтернет можуть бути використані суб'єктами запобігання злочинності у своїй практичній діяльності, зокрема, перспективним є розвиток використання соціальних Інтернет-мереж при здійсненні запобіжної діяльності на загальносоціальному, спеціально-криминологічному та індивідуальному рівнях.

Аналіз останніх досліджень і публікацій. Кримінологічними дослідженнями, що присвячені проблемам використання соціальних Інтернет-мереж для розслідування кримінальних правопорушень та запобігання злочинності займалися такі вчені, як: К. І. Беляков, В. М. Бутузов, В. Д. Гавловський, О. Ф. Гіда, А. І. Марущак, Д. М. Цехан, В. П. Шеломенцев та інші. Однак, розширення технологічних можливостей мережі Інтернет, суттєве збільшення кількості користувачів соціальних мереж як в Україні, так і світі, а також активізація спроб використання соціальних мереж зі злочинною метою, потребує проведення подальших кримінологічних досліджень у цьому напрямі.

Метою статті є дослідження сутності використання соціальних Інтернет-мереж для запобігання злочинності та розроблення відповідних практичних рекомендацій з цього питання.

Виклад основного матеріалу. Соціальними мережами у світі користуються близько 3,5 мільярдів людей [2, с. 3]. Станом на січень 2021 року в Україні було 25,70 мільйона користувачів соціальних мереж, що становить 58,9 % від загальної кількості населення. Кількість користувачів соціальних медіа в Україні зросла на 3,5 мільйона (+16%) між 2020 і 2021 роками [3]. Загалом у сучасному світі соціальні мережі є невід'ємною складовою комунікаційних процесів на всіх рівнях життєдіяльності соціуму. Вони стали зручним засобом отримання й передачі різноманітної інформації, що значно спростило соціальне буття людини та прискорило обмін інформацією між суб'єктами соціального простору [4].

Зокрема, за даними соціологічних досліджень щодо користувачів соціальної мережі «Facebook» було встановлено, що: 70 % опитаних відвідують свою сторінку соціальної мережі щодня; 80 % – відкрили доступ до перегляду даних зі своєї сторінки усім бажаючим; 60 % – використовують свою сторінку для підтримання зв'язків з друзями; 74 % – розміщують на своїй сторінці особисті дані, які повністю відповідають дійсності; 70 % – додають людей у список своїх друзів на своїй сторінці, спираючись на знайомство, чи на близькі дружні відносини з ними; лише 30 % опитаних не обмінюються і не планують обмінюватися на своїй сторінці соціальної мережі інформацією про вчинення протиправних діянь, шляхом використання повідомлень, хоча останні 70 % таку можливість не виключають при спілкуванні через Інтернет [5, с. 58].

Однак, соціальні Інтернет-мережі можуть також бути використанні зі злочинною метою, зокрема, шляхом збору коштів терористичними угрупованнями для фінансування тероризму. При цьому відбувається пропаганда тероризму та встановлення відповідних контактів зі своїми прихильниками [6]. В цьому процесі можуть бути задіяні до декількох тисяч «спонсорів» і, таким чином, можливо здійснення збору значних сум готівки. Часто збір коштів для підтримки тероризму й екстремізму здійснюється під виглядом законної благодійної або гуманітарної діяльності [7, с. 130–131].

Йще одним негативним прикладом використання соціальних Інтернет-мереж є кібербулінг – неодноразова поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований. Кібербулінг – це булінг із застосуванням цифрових технологій, він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах [8]. Кібербулінг в сукупності з іншими факторами може бути причиною прояву скулшутінгу – збройного нападу (найчастіше учня на школярів) у навчальному закладі. Одним з найбільш відомих вважається скулшутінг у школі «Колумбайн» в 1999 році (США). Двоє підлітків – Ерік Гарріс і Ділан Кліболд – планували підірвати школу, однак саморобні бомби не спрацювали, і тоді вони почали розстрілювати всіх, хто був у приміщенні, після чого вчинили самогубство. Усього загинуло 15 осіб, включно із самими стрільцями [9].

Особливістю скулшутінгу є те, що цей злочин може довго плануватися із висвітленням всього процесу підготовки або окремих його частин в соціальних мережах. В багатьох випадках, напередодні вчинення злочину, здійснюється опис «сценарію» розстрілу людей та викладається інша деталізована інформація кримінологічного змісту. Необхідно також зазначити, що інформацію про вчинення скулшутінгу деякі засоби масової комунікації інколи «повторно» використовують з метою досягнення певних цілей, насамперед фінансового змісту. При цьому використовується клікбейт (clickbait) – формування заголовків інформаційних повідомлень, що привертають увагу, переважно гіперболічного характеру для спонукання читачів натискати на посилення статті. Зокрема, часто використовується для отримання доходу від рекламодавців на основі кількості «кліків» стосовно певної статті. Клікбейт також використовується для залучення більшої аудиторії шляхом психо-

логічного впливу, оскільки певну частину людей приваблює так звана «шокова інформація» [10]. При цьому така інформація, що розповсюджується в соціальних Інтернет-мережах може спотворюватись, втрачати цілісність, мати елементи романтизації злочинної поведінки, що насамперед, негативно впливає на психіку неповнолітніх.

Йще одним негативним прикладом використання соціальних Інтернет-мереж є поширення інформації про так звані «групи смерті», які хоч і мають різну назву: «Синій кит», «Тихий дім», «Розбуди мене о 04:20», «Червона сова», «Момо» тощо, проте мають спільну мету – доведення до самогубства дитини, попередньо втягнутої до таких спільнот. Підвищена суспільна небезпека полягає в тому, що жертвами таких самогубств у 100 % випадків стають діти та підлітки [11, с. 218]. Необхідно зазначити, що з початку 2021 року до кінця квітня в Україні зафіксували 126 випадків підліткових самогубств або спроб самогубств [12], в той час як у 2020 році їх було 123, а в 2019 році – 111 [13].

Разом із цим, соціальні Інтернет-мережі можуть бути використані для запобігання злочинності та розслідування кримінальних правопорушень. Зокрема, вони є цінним джерелом криміналістичної інформації, яка може орієнтувати слідчого для прийняття тактичних рішень при розслідуванні кіберзлочинів. Криміналістична інформація у соціальній Інтернет-мережі являє собою сукупність даних, повідомлень та відомостей, про джерела й механізми виникнення ідеальних та матеріальних слідів, що мають відношення до злочинної події та отримані в мережі Інтернет із застосуванням спеціальних засобів, з метою встановлення обставин злочинної події у кримінальному провадженні. Криміналістичне дослідження інформації соціальних Інтернет-мереж відбувається у декілька етапів: 1) пошук та виявлення інформації; 2) збір; 3) зняття інформації; 4) дослідження інформації. Способами збору інформації із соціальних мереж є такі: а) інформаційно-аналітична робота; б) запити; в) використання спеціальних програм; г) створення «фейкових» сторінок та ін. [1, с. 143–144].

Важливим є також здійснення правоохоронного моніторингу соціальних мереж з метою виявлення не лише ознак кримінальних й адміністративних правопорушень, попередження, припинення та розкриття злочинів, а і відслідковування процесів деструкції соціальної злагоди (розпалювання національної, релігійної ворожнечі, поширення екстремістських та сепаратистських гасел тощо) з метою подальшого визначення їх загрози для

національної безпеки держави та вжиття відповідних упереджувальних заходів [14, с. 21].

Отже, враховуючи специфіку соціальних мереж, особливостей розміщеної користувачами інформації, способів та методів для її одержання, а також зарубіжний досвід використання інформації, яка міститься в соціальних мережах, правоохоронні органи мають можливість визначити основні напрями використання її у практичній діяльності для: отримання довідково-допоміжної інформації щодо конкретних осіб та їх контактів, стосовно конкретного кримінального провадження, свідків, потерпілих, підозрюваних; пошуку інформації щодо соціальних зв'язків правопорушників, їх каналів злочинних контактів; встановлення достовірності алібі, місця знаходження особи; підвищення рівня довіри громадськості до правоохоронних органів та ін. [15, с. 95].

Зокрема, використовуючи фотографії користувачів, які вони розміщують у своїх профілях соціальних мереж, таких як наприклад «Facebook» та «Instagram», можливо дуже швидко розширити та поповнити бази даних автоматизованих біометричних та інших систем, якими користуються працівники МВС України відносно осіб, що готують, вчиняють замах або вже вчинили кримінальне правопорушення чи ухиляються від досудового розслідування і суду. А це, в свою чергу, надасть і розширить працівникам правоохоронних органів наступні можливості: 1) маючи фотографію чи фоторобот правопорушника – швидко ідентифікувати його особу у тому випадку, якщо його фотографії є в базі даних автоматизованої біометричної чи іншої системи; 2) використати фотографії із списку «друзів» в сторінці соціальної мережі правопорушника з метою пред'явлення їх для впізнання потерпілому, або свідкам кримінального правопорушення, а також для впізнання самого потерпілого в разі його вбивства чи смерті; 3) наявність в базах даних автоматизованих біометричних систем багатьох фотографій однієї особи, але знятих з різних кутів та ракурсів дозволить ідентифікувати особу краще, якісніше й ефективніше, ніж використати звичайні обліки фотографій МВС, що зменшить чи унеможливить судову помилку; 4) під час проведення оперативно розшукового заходу дозволить більш повно та швидко встановити коло контактів і зв'язків особи; 5) вказаний перелік не обмежує й інші можливості [5, с. 58–59].

Загалом, використання соціальних Інтернет-мереж для отримання кримінологічно значимої інформації можна співставити з поняттям провадження розвідки на основі відкритих джерел –

Open source intelligence (OSINT), тобто концепцією, методологією і технологією добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. При цьому розвідка на основі відкритих джерел широко здійснюється в мережі Інтернет, це зокрема: онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, вміст, створений користувачами), YouTube та інші відео-хостинги, вікі-довідники та інші вебсайти соціальних медіа (наприклад, Facebook, Twitter, Instagram та ін.) [16].

При цьому інформація із соціальних Інтернет-мереж є частиною так званого «цифрового сліду» особи, дослідження якого може суттєво сприяти розслідуванню кримінальних правопорушень, оскільки містить широкий спектр інформації як безпосередньо про особу так і про її оточення [17]. Індивідуальний цифровий слід (відбиток) особи в мережі Інтернет – Digital Footprint інколи йще називають цифровим татуванням – Digital Tattoo [18]. Загалом цифрові сліди можна класифікувати на два різних типи: 1) активні цифрові сліди – вся інформація, яку користувач спеціально розміщує в мережі Інтернет (наприклад, дані розміщені в соціальних мережах); 2) пасивні цифрові сліди – це інформація, що розміщена та зібрана в мережі Інтернет без відома користувача (наприклад, інформація розміщена в результаті Інтернет-покупок) [19].

Висновки. Отже, вирішення проблем запобігання злочинності в сучасних умовах розвитку інформаційно-комунікаційних технологій потре-

бує проведення відповідних наукових досліджень та загалом переосмислення кримінологічних підходів у цій сфері (в тому числі, щодо запобігання кіберзлочинності, тероризму, кібербулінгу, розповсюдженню дитячої порнографії тощо). При цьому можна сформулювати наступні напрями використання можливостей соціальних Інтернет-мереж для запобігання злочинності: здійснення моніторингу та аналізу кримінологічно значимої інформації для прогнозування злочинності; розроблення та впровадження відповідних запобіжних заходів на загальносоціальному, спеціально-кримінологічному та індивідуальному рівнях; підвищення рівня комунікації між поліцією і громадянами щодо вирішення проблем запобігання злочинності; використання соціальних Інтернет-мереж для поширення оперативної інформації, щодо розшуку злочинців, повідомлень про вчинені кримінальні правопорушення та можливої небезпеки для мешканців певних територій; інформаційної підтримки в соціальних Інтернет-мережах об'єднань громадян, що визначають пріоритетом в своїй діяльності запобігання злочинності безпосередньо в місцях свого проживання (сусідський нагляд) та ін. Важливим є також розроблення інтерактивного блогу запобігання злочинності з метою налагодження в соціальних Інтернет-мережах комунікаційного зв'язку між працівниками правоохоронних органів (дільничними офіцерами поліції) та мешканцями певних визначених територій щодо обговорення та вирішення проблем запобігання злочинності на локальному рівні (селище, мікрорайон).

Список літератури:

1. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми (С. 142–146). *Кримінальні загрози в секторі безпеки: практики ефективного реагування* : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право», м. Харків, 26 верес. 2019 р. / редкол.: В. Я. Тацій, Ю. Г. Барабаш, Б. М. Головкін, О. В. Таволжанський. Харків : Право, 2019. 176 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf (дата звернення: 21.06.2022).
2. Робота із соціальними мережами: посібник з питань використання соціальних мереж, розроблений Департаментом преси і публічної інформації Консультативної місії ЄС в Україні. м. Київ, 2020 р. 45 с. URL: <https://www.euam-ukraine.eu/wp-content/uploads/2020/09/Working-with-Social-Media-Compendium-ukrainian-august-2020-for-publication.pdf> (дата звернення: 21.06.2022).
3. Kemp S. Digital 2021 – Ukraine. URL: <https://datareportal.com/reports/digital-2021-ukraine> (дата звернення: 21.06.2022).
4. Битяк Ю. П., Калиновський Ю. Ю. Деструктивний вплив соціальних мереж на інформаційну безпеку людини й суспільства. *Науковий семінар ХНУ ПС ім. І. Кожедуба, 21 жовтня 2020*. URL: <http://www.hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-vijna-gumanitarnij-aspekt-21-10-2020/3.pdf> (дата звернення: 21.06.2022).
5. Юхно О. О., Загуменний О. О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Видання друге, доп. і перероб. (Серія «Бібліотека слідчого і детектива: проблеми кримінального процесу») Харків : Колегіум, 2020. 116 с. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9871/Vykorystannia%20suchasnykh%20informatychnykh%20tekhnohii_Yukhno_Zahumennyi_2020.pdf?sequence=1&isAllowed=y (дата звернення: 21.06.2022).

6. Emerging Terrorist Financing Risks. URL: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html> (дата звернення: 21.06.2022).
7. Типологічні дослідження Державної служби фінансового моніторингу України за 2017 рік К., 2018. 148 с. URL: https://finmonitoring.in.ua/wp-content/uploads/2018/04/180410_1446_book_ua_topology_sfs.pdf (дата звернення: 21.06.2022).
8. Кібербулінг – що це та як це зупинити? URL: <https://www.unicef.org/ukraine/cyberbullying> (дата звернення: 21.06.2022).
9. Скібіцька Ю. Натхненні «Колумбайном». URL: <https://zaborona.com/nathnenni-kolumbajnom-rozpovidayemo-pro-fenomen-skulshutinga-koly-shkolyari-vbyvayut-inshyh-shkolyariv> (дата звернення: 21.06.2022).
10. The Art Of Clickbait. URL: <https://somiibo.com/blog/the-art-of-clickbait/> (дата звернення: 21.06.2022).
11. Павленко С. Тактика запобігання доведенню неповнолітніх до самогубств через соціальні мережі (інтернет-спільноти): сучасні вітчизняні реалії та зарубіжний досвід. *Підприємництво, господарство і право*. 2018. № 11. С. 217–225. URL: <http://pgp-journal.kiev.ua/archive/2018/11/42.pdf> (дата звернення: 21.06.2022).
12. За перші чотири місяці 2021-го в Україні сталося 126 підліткових самогубств або спроб – Денісова. URL: <https://www.radiosvoboda.org/a/news-denisova-pislitkova-samohubstva/31278009.html> (дата звернення: 21.06.2022).
13. Генпрокуратура констатувала сплеск спроб суїциду серед українських підлітків. URL: https://lb.ua/pravo/2021/05/14/484645_genprokurorka_konstatuvala_splesek.html (дата звернення: 21.06.2022).
14. Гавловський В. Д. Правоохоронний моніторинг соціальних мереж. *«Правова інформатика»*, 2014. № 3(43). С. 19–25. URL: <http://ippi.org.ua/sites/default/files/14gvdmsm.pdf> (дата звернення: 21.06.2022).
15. Косолап О. В. Використання соціальних мереж у виявленні та розслідуванні злочинів: зарубіжний досвід та перспективні напрямки. *«Young Scientist»*. 2016. № 8 (35). С. 93–96. URL: <http://molodyvcheny.in.ua/files/journal/2016/8/21.pdf> (дата звернення: 21.06.2022).
16. Розвідка на основі відкритих джерел. URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел (дата звернення: 21.06.2022).
17. Klippenstein L. Social Media and Criminal Investigations: Public content and its role in solving crimes. URL: <https://www.lawnw.org/social-media-and-criminal-investigations-public-content-and-its-role-in-solving-crimes/> (дата звернення: 21.06.2022).
18. Digital Footprint (Digital Tattoo). URL: <https://dpi.wi.gov/internet-safety/digital-footprint> (дата звернення: 21.06.2022).
19. Mudrakola S. Digital footprints: control how much the Internet knows about you. URL: <http://techgenix.com/digital-footprints-control/> (дата звернення: 21.06.2022).

Bugera O.I. SOCIAL INTERNET NETWORKS AND PROBLEMS OF CRIME PREVENTION IN MODERN CONDITIONS OF INFORMATION TECHNOLOGY DEVELOPMENT

The article examines the problems of using social Internet networks to prevent crime in modern conditions of development of information and communication technologies. It is established that the solution of problems of crime prevention, in the conditions of constant development of information and communication technologies requires carrying out of the corresponding scientific researches and in general rethinking of criminological approaches in this sphere. The potential danger of using social Internet networks for criminal purposes was emphasized, in particular, regarding: committing cybercrimes; fundraising by terrorist groups for financing and propaganda of terrorism, attraction of new members of terrorist organizations; cyberbullying; distribution of child pornography; dissemination (primarily among minors) of information on so-called «death groups» aimed at leading to the suicide of a child previously involved in such communities, etc. The directions of using the possibilities of social Internet networks for crime prevention have been formed, in particular: monitoring and analysis of criminologically significant information for crime forecasting; development and implementation of preventive measures at the general social, special criminological and individual levels; increasing the level of communication between the police and citizens on solving crime prevention problems; use of social Internet networks to disseminate operational information on the search for criminals, reports of criminal offenses and possible dangers for residents of certain areas; information support in social Internet networks of citizens' associations, which prioritize crime prevention in their activities directly in their places of residence (neighborhood supervision), etc. It is also important to develop an interactive crime prevention blog in order to establish communication on social Internet networks between law enforcement officers (police officers) and residents of certain areas to discuss and address crime prevention at the local level (village, neighborhood).

Key words: Internet, social Internet networks, information technologies, crime, prevention.