

УДК: [316.472.4:004.738.5]: 343.98.06

DOI: <https://doi.org/10.32366/2709-9261-2022-3-1-49-56>

Павлиш Тетяна Григорівна,
кандидат педагогічних наук
(Донецький державний університет
внутрішніх справ, м. Кривий Ріг)
ORCID: <https://orcid.org/0000-0002-5288-5301>

Терещенко Олександр Олександрович,
викладач
(Донецький державний університет
внутрішніх справ, м. Кривий Ріг)
ORCID: <https://orcid.org/0000-0003-0762-7546>



АНАЛІЗ ІНФОРМАЦІЇ ІЗ СОЦІАЛЬНИХ МЕРЕЖ ПІД ЧАС РОЗСЛІДУВАННЯ ТА В ХОДІ ПРОТИДІЇ ЗЛОЧИНАМ

Статтю присвячено дослідженню проблем використання соціальних мереж в інтернеті для виявлення значимої інформації під час розслідування злочинів та в ході протидії їм. Розглянуто переваги й недоліки спілкування в соціальних мережах. Розкрито роль правоохоронного моніторингу й аналізу профілей осіб у соціальних мережах. Наголошено на актуальних проблемах та ризиках використання соціальних мереж,

комплексному аналізу соціальних мереж як джерела криміналістичної інформації під час розслідування злочинів.

Ключові слова: соціальна мережа; розслідування злочинів; кіберпростір; інформаційне середовище.

Постановка проблеми. Нині соціальні мережі є популярними, вони диктують нові правила комунікації та нові підходи до роботи з інформацією, у тому числі у сфері протидії злочинності. На сьогодні кількість користувачів соціальних медіа становить понад 3 млрд. Віртуальне спілкування отримало глобальне поширення, 75 % людей мають свої профілі в Instagram, Facebook, YouTube та ін.

Соціальні мережі є невід'ємним елементом спілкування більшості учасників онлайн-комунікації. Через них користувачі здобувають альтернативні до традиційних медіа факти, коментують, інтерпретують і поширюють їх, стаючи таким способом співучасниками процесу. Безумовно, основним фактором підвищеної уваги до соціальних мереж є інформація, яка в них циркулює [1].

Варто зазначити, що більшість інформаційної діяльності злочинців перенесено у віртуальний світ.

Аналіз останніх досліджень і публікацій. Окремі аспекти використання соціальних мереж під час розслідування та в ході протидії злочинам розглянуто

в наукових працях К. А. Автухова, Р. І. Благуті, О. І. Бугери, О. М. Дуфенюк, А. В. Мовчана, В. М. Шевчук та інших.

О. М. Дуфенюк у своєму дослідженні наголошує на тому, що успішне використання соціальних мереж у правоохоронній діяльності передбачає насамперед розуміння механізму функціонування таких платформ для комунікації, кожна з яких має свій набір опцій та задач, які вона покликана вирішувати [2, с. 57].

Як зауважують науковці Р. І. Благута, А. В. Мовчан, на сьогодні використання кіберпростору в попередженні та розкритті злочинів є перспективним напрямом. Учені вважають можливим використовувати інтернет-мережу для виявлення осіб, які становлять оперативний інтерес; пошуку конкретних осіб, установлення їх фізичного місцезнаходження; налагодження негласних зв'язків із подальшим входженням у безпосередній контакт; пошуку викрадених речей; здійснення психологічного впливу на учасників кримінальних структур шляхом ведення активної роботи на форумах і чатах [3, с. 166].

Формування цілей (постановка завдання). Метою статті є дослідження можливостей збору інформації із соціальних мереж під час розслідування та в ході протидії злочинам.

Виклад основного матеріалу. На сучасному етапі світового розвитку набуває нового значення інтернет-мережа й усе, що з нею пов'язано. Суспільство наблизилося до того, що інтернет став основним генератором глобальних або всесвітніх макротенденцій. Він сприяє трансформації ціннісних орієнтирів людства та його соціальних структур. Останнім часом важко уявити своє життя без інтернету. Він міцно утвердився в нашому побуті: ми активно користуємося інтернетом удома, на роботі, з удосконаленням новітніх або інноваційних технологій інтернет став головною функцією мобільних телефонів і смартфонів, що дало можливість практично весь час перебувати онлайн.

Поява інтернету радикально змінила форми, зміст, механізми, функції соціальних комунікацій. Із розвитком інтернету з'явилася можливість використовувати всі його досягнення в різних їх проявах. Одним із таких проявів стали соціальні мережі, які набули на сьогодні статусу невід'ємного атрибута нашого життя. Уявити сучасну людину без соціальних мереж просто неможливо [4]. Спілкування, пошук інформації і друзів, обмін новинами, можливість слухати музику, дивитися відео і фотографії – усе це, здається, завжди було. Складно усвідомити, що колись люди могли обійтися без профілю в соціальній мережі.

Розглянемо визначення поняття «соціальна мережа», подане в різних наукових джерелах. Соціальна мережа – це: 1) інтернет-сервіс, призначений одночасно для комунікації користувачів і для розміщення та поширення ними інформації [5, с. 236]; 2) соціальна структура, що утворена індивідами або організаціями; в інтернеті соціальні мережі мають вигляд сайтів, на яких користувачі можуть створювати персональні сторінки та спільноти для спілкування і поширення інформації серед великої кількості людей [4]; 3) соціальна структура, утворена індивідами або організаціями, що відображає розмаїті зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними зв'язками [6].

Кіберпростір характеризується трьома основними ознаками: це інформаційний простір; він є комунікативним середовищем; утворюється за

допомогою технічних систем. Використання соціальних мереж має на меті насамперед соціалізацію, прагнення особистості до встановлення стосунків з іншими користувачами. Соціальні мережі – це певне комунікативне середовище, що сприяє швидкому обміну інформацією, надає можливість особі бути в центрі подій, отримувати позитивні враження від нових знайомств та ін.

Негативними сторонами соціальних мереж є те, що останнім часом кіберпростір все частіше стає місцем та безпосередньо інструментом злочину.

Р. І. Благута, А. В. Мовчан виділяють низку проблем, пов'язаних із використанням інформації в інтернет-мережі: зареєстровані непоодинокі випадки, коли соціальні мережі сприяють учиненню злочинів (наприклад, особа повідомляє в мережі, що поїхала у відпустку, а в цей час її житло грабують); соціальні мережі несуть певну загрозу ще й тому, що злочинці також спілкуються через них, створюють закриті групи; у мережі міститься багато недостовірної інформації [3, с. 167].

Користувачі активно розміщують на своїх сторінках інформацію особистого характеру: номери телефонів, адреси, місце роботи, посаду, місце свого знаходження, фотографії, плани на майбутнє, що загрожує самим користувачам та значно звужує коло потенційних жертв для зловмисників. Ураховуючи зазначені характеристики соціальних мереж, сучасні тенденції використання інтернет-простору для вчинення злочинних діянь та неабияку роль, яка належить цій категорії як чиннику розвитку суспільства в цілому, виникає необхідність створення державного механізму протидії використанню соціальних мереж злочинними елементами, що покладатиме на правоохоронні органи виконання нових обов'язків та потребуватиме від працівників оволодіння новими теоретичними та практичними навичками [7].

О. М. Дуфенюк виокремлює такі блоки знань про соціальні мережі (далі – СМ), які необхідні працівнику поліції:

- інформація СМ використовується злочинцями для вчинення злочинів;
- інформація СМ може бути використана для притягнення до відповідальності осіб;
- інформація СМ може бути використана для попередження злочинів;
- СМ можуть бути використані поліцейськими для реалізації пошукових цілей;
- СМ можуть бути використані для інформаційно-роз'яснювальних цілей;
- СМ можуть бути використані для формування позитивного іміджу правоохоронних органів [2].

В Україні забезпечення онлайн-безпеки кожного громадянина нашої держави покладається на кіберполіцію – один із структурних підрозділів Національної поліції, який діє у складі кримінальної поліції та спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем [8].

Моніторинг правоохоронцями соціальних мереж, як зазначає В. Д. Гавловський, може включати:

- автоматичне комп'ютерне спостереження, що має проводитися з використанням відповідного програмного забезпечення і спрямовуватися на

пошук у соціальних мережах за ключовими словами чи змістом інформації, яка містить: пропаганду суспільно небезпечних ідей; відомості з обмеженим доступом; домовленості про спільні злочинні дії; відомості щодо збуту або придбання товарів і предметів, заборонених для відкритого обігу, майна, здобутого злочинним шляхом; надання заборонених послуг; торгівлі людьми;

- заходи, пов'язані із залученням громадськості до отримання інформації про використання соціальних мереж у деструктивних цілях;

- оперативно-пошукові заходи щодо забезпечення оперативної закупівлі та (або) контрольованого постачання товарів, заборонених для відкритого обігу, майна, здобутого злочинним шляхом, надання заборонених послуг, торгівлі людьми через соціальні мережі;

- оперативне впровадження у віртуальні соціальні групи, що мають деструктивні цілі, з метою отримання інформації про їх персональний склад, місця зустрічей, плани та засоби, що використовуються в деструктивній діяльності;

- оперативно-аналітичні заходи, спрямовані на прогноз розвитку ситуації, розробка заходів з утримання її під контролем, отримання нових даних про суб'єктів деструктивної діяльності, їх зв'язки, місця відвідування, злочинні наміри тощо;

- заходи оперативно-технічного характеру, спрямовані на виявлення та локалізацію комп'ютерних засобів (та їх користувачів), що стали джерелами (засобами) розповсюдження в соціальних мережах інформації деструктивного характеру [9].

Аналіз інформації, розміщеної в соціальних мережах, може допомогти під час розслідування багатьох злочинів у пошуку невідомих слідству джерел інформації. Варто зазначити, що в кіберпросторі слідчі підрозділи Національної поліції України можуть виявити осіб, які становлять оперативний інтерес, знайти конкретних осіб за профілями в соціальних мережах через пошук фото і проаналізувати його, здійснити пошук і відслідковування кола осіб, які вчиняли злочинні дії, використовуючи інтернет-мережу. Звичайно, що під час розслідування злочину можна проаналізувати й телефонні контакти потерпілої особи. Наприклад, перевірити будь-який телефонний номер у Viber: якщо він зареєстрований у цій спільноті, то обов'язково отримаємо фото профілю і в деяких випадках дату народження, прізвище та ім'я, електронну адресу. Далі слід знайти фото шляхом пошуку за зображенням у Google. Так можна побачити: результати пошуку, пов'язані з об'єктами на зображенні; подібні зображення; вебсайти, на яких розміщено це фото або схожі зображення.

Правоохоронці на підставі відповідного аналізу наявної інформації можуть отримати необхідні дані про місцеперебування конкретної особи як під час вчинення злочину, так і під час здійснення спеціальних заходів щодо розшуку осіб, які переховуються від органів досудового розслідування та суду. Використання такої інформації дозволяє встановити коло осіб, з якими спілкується особа, що розшукується, її інтереси та захоплення, місця можливого перебування, установити контроль за її пересуванням тощо [10].

Аналіз профілей користувачів у соціальних мережах відбувається за такою схемою:

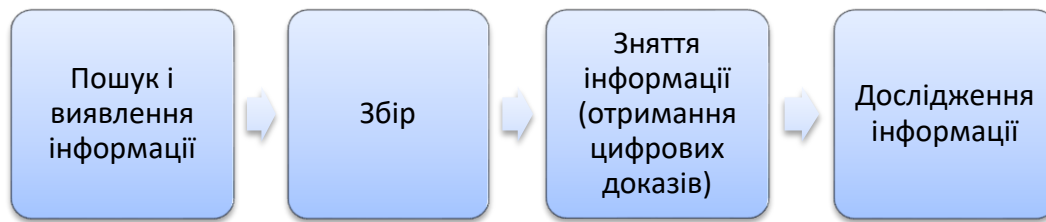


Рис. 1. Етапи криміналістичного аналізу інформації в соціальних мережах

Інформаційно-аналітична робота зі збору інформації про користувачів соціальних мереж дає змогу отримати важливі дані для викриття осіб, які займаються неправомірною діяльністю. Так, аналізуючи найбільш популярні соціальні мережі серед користувачів, можна отримати такі дані: 1) Facebook – ім'я, унікальний код (ID), геолокацію, коло друзів, підписників, пристрій, який використовувала особа, час активності; 2) Twitter – ім'я, назву облікового запису, унікальний код (ID), підписників, місцезнаходження користувача, а також пристрій, з якого були зроблені записи; 3) Instagram – ім'я користувача, назву облікового запису, кількість та імена підписників, верифікаційний статус; 4) YouTube – ім'я користувача, назву каналу, кількість підписників, дату та час викладених матеріалів [10].

Слід зауважити, що аналіз профілей соціальних інтернет-мереж не тільки дозволяє виявити коло друзів, інтереси і вподобання, місцезнаходження досліджуваної особи, перелік запланованих для відвідування заходів, а й скласти соціально-психологічну характеристику особи користувача.

Інформація із соціальних мереж може орієнтувати слідчого щодо прийняття тактичних рішень під час розслідування кіберзлочинів і злочинів узагалі. Нерідко злочинці хизуються результатом своїх неправомірних дій та фіксують свою злочинну діяльність. Інформація, що міститься на персональних сторінках соціальних мереж, дає змогу ідентифікувати особу злочинця, обстановку, місце події, співучасників, знаряддя, допомагає виявити важливі обставини, що мають значення у кримінальному провадженні [11].

Правоохоронними органами постійно здійснюється моніторинг підозрілих блогів, чатів, сайтів. Прикладом використання відкритих джерел інформації в інтернеті є пошукова мережа «Bellingcat», розроблена в Амстердамі. За аналізом фотографій, розміщених у соцмережах, «Bellingcat» змогла визначити точне місце розташування злочинця-втікача, який переховувався від поліції Нідерландів. Злочинець активно постив фотографії в соцмережах, закликаючи поліцію «зловити його, якщо зможуть». Проаналізувавши десятки фотографій та зіставивши отриману інформацію з відкритими джерелами, фахівцям вдалося встановити будинок, де проживав злочинець, на острові Кіш у Перській затоці.

Дослідницька пошукова мережа «Bellingcat» наголошує на тому, що для аналізу контенту достатньо критичного підходу та ретельного вивчення контексту зображення або посту в поєднанні з такими простими інструментами, як пошук у Google або на інших платформах зворотного пошуку зображень.

Висновки. Отже, використання можливостей інтернет-мережі є процесом, що постійно триває, а тому має бути предметом дослідження кримінологічної

науки з метою вироблення підходів щодо запобігання злочинності в якісно нових умовах обміну інформацією. Аналіз соціальних мереж може вирішити багато питань під час розкриття та в ході протидії злочинам, але для цього оперативні і слідчі підрозділи правоохоронних органів потребують відповідних спеціалістів з інформаційно-комп'ютерних технологій. Застосування сучасних інформаційних технологій, соціальних мереж під час розслідування злочинів і викриття злочинця залишається актуальним напрямом для подальшого детального дослідження та аналізу в діяльності правоохоронних органів.

Список використаних джерел

1. Гіда О. Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір. URL: http://webcache.googleusercontent.com/search?q=cache:fzee15s5q00J:irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAG E_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF/boz_2013_3 (дата звернення: 24.01.2022).
2. Дуфенюк О. М. Використання соціальних мереж у протидії злочинності – нові виклики і нові можливості. *Напрями реформування кримінальної юстиції в Україні*: матеріали науково-практичного семінару (м. Львів, 22 травня 2020 р.). Львів: Львівський державний університет внутрішніх справ, 2020. С. 56–61. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/22_05_2020.pdf (дата звернення: 22.01.2022).
3. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
4. Соціальні мережі: різні аспекти впливу на людину. *Українське право*. URL: https://ukrainepраво.com/legal_publications/essay-on-it-law/it_law_berkiy_Social_networks_and_there_involves/ (дата звернення: 02.02.2022).
5. Радейко Р. І. Соціальні мережі як об'єкт правового регулювання. URL: <http://aphd.ua/publication-144/> (дата звернення: 25.01.2022).
6. Соціальна мережа. URL: https://uk.wikipedia.org/wiki/Соціальна_мережа (дата звернення: 25.01.2022).
7. Косолап А. В. Соціальні мережі як об'єкт криміналістичного дослідження. URL: https://vkslaw.knu.ua/images/verstka/1_2016_Kosolap.pdf (дата звернення: 22.01.2022).
8. Офіційний сайт кіберполіції України. URL: <https://cyberpolice.gov.ua/contacts/> (дата звернення: 27.01.2022).
9. Гавловський В. Д. Теоретичні засади відстеження деструктивних процесів у соціальних мережах. URL: <http://pravoznavec.com.ua/period/article/27006/%C3> (дата звернення: 08.02.2022).
10. Лисенко О. В. Використання інформаційних технологій для розшуку осіб, які переховуються від органів досудового розслідування та суду. *Науковий вісник Національного університету ДПС України*. 2014. № 2 (65). С. 194–201.
11. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf (дата звернення: 28.01.2022).
12. Бугера О. І. Соціальні інтернет-мережі та запобігання злочинності: сучасні тенденції. URL: <http://socio-journal.kpi.kiev.ua/archive/2018/2/18.pdf> (дата звернення 28.01.2022).

References

1. Hida, O. F. Sotsialni merezhi yak zasib destruktivnykh vplyviv cherez informatsiyni prostir [Social networks as a means of destructive influences through the information space]. URL: http://webcache.googleusercontent.com/search?q=cache:fzee15s5q00J:irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAG E_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF/boz_2013_3 (data zvernennia: 24.01.2022) [in Ukrainian].
2. Dufeniuk, O. M. (2020). Vykorystannia sotsialnykh merezh u protydii zlochyynnosti – novi vyklyky i novi mozhlyvosti [The use of social networks in the fight against crime – new challenges and new opportunities]. *Napriamy reformuvannia kryminalnoi yustytzii v Ukraini*: materialy naukovo-praktychnoho seminaru (m. Lviv, 22 travnia 2020 r.). Lviv: Lvivskiy derzhavnyi universytet

- vnutrishnikh sprav. S. 56–61. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/22_05_2020.pdf (data zvernennia: 22.01.2022) [in Ukrainian].
3. Blahuta, R. I., Movchan, A. V. (2020). Novitni tekhnolohii u rozsliduvanni zlochyniv: suchasnyi stan i problemy vykorystannia : monohrafiia [The latest technologies in the investigation of crimes: the current state and problems of use : a monograph]. Lviv : LvDUVS. 256 s. [in Ukrainian].
 4. Sotsialni merezhi: rizni aspekty vplyvu na liudynu [Social networks: various aspects of human impact]. *Ukrainske pravo*. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_berkiy_Social_networks_and_there_involves/ (data zvernennia: 02.02.2022) [in Ukrainian].
 5. Radeiko, R. I. Sotsialni merezhi yak ob'ekt pravovoho rehuliuвання [Social networks as an object of legal regulation]. URL: <http://aphd.ua/publication-144/> (data zvernennia: 25.01.2022) [in Ukrainian].
 6. Sotsialna merezha [Social network]. URL: https://uk.wikipedia.org/wiki/Sotsialna_merezha (data zvernennia: 25.01.2022) [in Ukrainian].
 7. Kosolap, A. V. Sotsialni merezhi yak ob'ekt kryminalistychnoho doslidzhennia [Social networks as an object of forensic research]. URL: https://vkslaw.knu.ua/images/verstka/1_2016_Kosolap.pdf (data zvernennia: 22.01.2022) [in Ukrainian].
 8. Ofitsiynyi sait kiberpolitsii Ukrainy [Official site of the cyber police of Ukraine]. URL: <https://cyberpolice.gov.ua/contacts/> (data zvernennia: 27.01.2022) [in Ukrainian].
 9. Havlovskiy, V. D. Teoretychni zasady vidstezhennia destruktyvnykh protsesiv u sotsialnykh merezhakh [Theoretical principles of tracking destructive processes in social networks]. URL: <http://pravoznavec.com.ua/period/article/27006/%C3> (data zvernennia: 08.02.2022) [in Ukrainian].
 10. Lysenko, O. V. (2014). Vykorystannia informatsiinykh tekhnolohii dlia rozshuku osib, yaki perekhovuiut vid orhaniv dosudovoho rozsliduvannia ta sudu [Use of information technology to search for persons hiding from pre-trial investigation and court]. *Naukovyi visnyk Natsionalnoho universytetu DPS Ukrainy*. № 2 (65). S. 194–201 [in Ukrainian].
 11. Shevchuk, V. M. Vykorystannia informatsii iz sotsialnykh internet-merezh pry rozsliduvani kiberzlochyniv: kryminalistychni problemy [The use of information from social networks in the investigation of cybercrime: forensic problems]. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf (data zvernennia 28.01.2022) [in Ukrainian].
 12. Buhera, O. I. Sotsialni internet-merezhi ta zapobihannia zlochynnosti: suchasni tendentsii [Social Internet Networks and Crime Prevention: Current Trends]. URL: <http://socio-journal.kpi.kiev.ua/archive/2018/2/18.pdf> (data zvernennia 28.01.2022) [in Ukrainian].

Pavlysh Tetiana,

PhD in Pedagogical Sciences

(Donetsk State University of Internal Affairs, Kryvyi Rih)

ORCID: <https://orcid.org/0000-0002-5288-5301>

Tereshenko Oleksandr,

Lecturer

(Donetsk State University of Internal Affairs, Kryvyi Rih)

ORCID: <https://orcid.org/0000-0003-0762-7546>

USE OF SOCIAL NETWORKS IN INVESTIGATION AND COMBATING CRIMES

The article is devoted to the study of the problems of using social networks on the Internet to identify relevant information in the investigation of crimes and their counteraction. The advantages and disadvantages of communication in social networks are considered. The role of law enforcement monitoring and analysis of profiles of persons in social networks is revealed. Emphasis is placed on current problems and risks of using social networks, comprehensive analysis of social networks as a source of forensic information in the investigation of crimes. In cyberspace, investigative units of the National Police of Ukraine can identify people of operational interest, find specific people by profiles on social networks by searching for and analyzing a photo, search and track the circle of people who committed crimes using the Internet. Information and analytical work on collecting information about users of social networks allows to obtain important data for exposing persons engaged in illegal activities. Analysis of profiles of social Internet networks not only allows you to identify friends and interests and preferences, location of the subject, the list of events planned to visit, but also to make a socio-psychological characteristics of the user. Information from social networks can guide the investigator to make tactical decisions in the investigation of cybercrime and crime. The use of the Internet is an ongoing process and should therefore be the subject of criminological research in order to develop approaches to crime prevention in a qualitatively new environment for the exchange of information. Suspicious blogs, chats and websites are constantly monitored by law enforcement

agencies. Analysis of social networks can solve many issues in the detection and fight against crime, but it requires appropriate specialists in information and computer technology in operational and investigative units of law enforcement agencies. The use of modern information technology, social networks in criminal further detailed research and analysis in the activities of law enforcement agencies.

Key words: *social network; crime investigation; cyberspace; information environment.*

Надіслано до редколегії 12.04.2022
Рекомендовано до публікації 18.04.2022