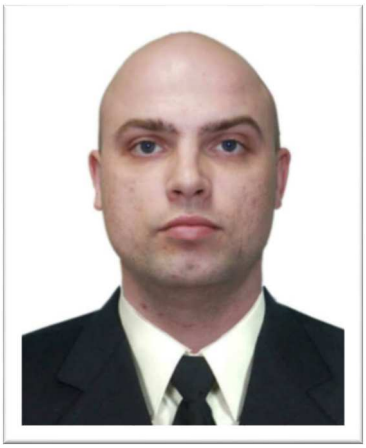
УДК: 343.98
DOI: https://doi.org/10.32366/2523-4269-2020-73-4-144-155

Одерій Олексій Володимирович,
доктор юридичних наук, доцент
(Донецький юридичний інститут МВС України, м. Маріуполь)
ORCID:https://orcid.org/0000-0002-6999-4387

Кожевніков Олексій Андрійович,
аспірант
(Харківський національний університет внутрішніх справ МВС України, м. Харків)
ORCID:https://orcid.org/0000-0001-8976-0863



ОТРИМАННЯ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ ШЛЯХОМ АНАЛІЗУ ВІДКРИТИХ ІНТЕРНЕТ-ДЖЕРЕЛ

Протидія злочинним проявам у сучасних реаліях потребує своєчасного та ефективного криміналістичного забезпечення розкриття і розслідування злочинів. Ця мета реалізується завдяки всебічному використанню досягнень сучасної науки й техніки, практичному опануванню новітніх технологій. У статті розглянуто технологію OSINT (Open source intelligence), яка являє собою розвідку на основі відкритих джерел. На підставі проведеного аналізу доведено, що вона може бути успішно використана правоохоронними органами для вирішення специфічних криміналістичних завдань. Наведено приклади застосування онлайн-сервісів з пошуку осіб, зафіксованих на фото- або відеозображеннях за антропометричними даними. Визначено шляхи використання отриманої медійної інформації як доказу в кримінальних провадженнях.

Ключові слова: *технології отримання інформації; криміналістично значуща інформація; соціальні мережі; кримінальне правопорушення; аналіз даних; OSINT; ідентифікація за ознаками зовнішності; портретні та фототехнічні дослідження.*

Постановка проблеми. Стрімкий розвиток цифрових засобів фото- та відеофіксації, їхня доступність у придбанні для пересічного громадянина зумовили появу великої кількості медійних файлів, що відтворюють об'єктивну обстановку в різних інтервалах часу та простору. Змістом такого контенту дедалі частіше стають фото або відеозаписи (навіть із місць скоєння правопорушень) з відображенням на них: а) осіб, що їх вчинили; б) механізму (способу) вчинення; в) транспортних засобів, які були задіяні; г) інших обставин, які мають значення для розкриття та розслідування кримінальних правопорушень.

До того ж інтернет-ресурси містять велику кількість різного виду інформації, де у популярних соціальних мережах («Інстаграм», «Фейсбук», «Вконтакті», «Однокласники» та інших) практично завжди наявна інформація про фізичну особу. Це пов'язано з тим, що громадяни за власною ініціативою та виключно на добровільній основі розміщують свої персональні дані (ПІБ, дату народження, місце проживання, коло спілкування, інтереси,

особисті побутові фотознімки та відеозаписи), створюючи тим самим потужний інформативний масив цифрових даних, що містять антропометричні ознаки зовнішності людини, анкетні дані, зображення місць фактичного проживання тощо. Наявність такої інформації (саме у відкритому доступі) надає можливість правоохоронним органам безперешкодно використовувати останню в оперативних цілях, оскільки результати її аналізу дають змогу отримувати орієнтуючу інформацію, а інколи й відразу ідентифікувати особу. Проте наукових спроб щодо вивчення можливостей використання загальнодоступних технологій отримання та аналізу відкритої інтернет-інформації у протидії злочинності немає.

Аналіз останніх досліджень і публікацій. Особливості використання спеціальних технологій задля отримання певної інформації саме з відкритих джерел вже були в колі інтересів окремих дослідників, таких як: О. О. Кожушко («Розвідка відкритих джерел інформації у розвідувальній практиці США») [1], О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов («Використання технології OSINT для отримання розвідувальної інформації») [2], О. Г. Додонов, Д. В. Ланде, В. Г. Путятін («Застосування OSINT в аналітичній діяльності») [3], Я. М. Жарков, А. О. Васильєв («Наукові підходи щодо визначення суті розвідки з відкритих джерел») [4]. Водночас практика свідчить, що медіа-спільнота останнім часом доволі активно використовує згадувані технології у своїй професійній діяльності. Так, журналісти інтернет-видання «Bellingcat» (засноване британським журналістом і блогером Еліотом Гіґґінсом) вже мають конкретні приклади розслідування резонансних подій безпосередньо шляхом аналізу відкритого інтернет-контенту (відеозаписів, карт, фотографій та ін.) [5], одним із яких є розслідування трагедії літака Boeing 777-200ER, яка відбулася в липні 2014 року в Донецькій області (рейс MH17) [6]. Аналогічні технології є головним джерелом інформації і для центру «Миротворець» [7].

Метою статті є аналіз та визначення сучасних можливостей використання альтернативних технологій автоматичної ідентифікації особи людини за елементами зовнішності правоохоронними органами України та окреслення подальших перспектив такої діяльності.

Виклад основного матеріалу. Забезпечення безпеки громадян і держави загалом неможливе без постійно здійснюваної правоохоронними органами діяльності у протидії злочинності, де важливу роль відіграє оперативне отримання криміналістично значущої інформації. Специфічною рисою сучасного суспільства є той факт, що значний обсяг такої інформації циркулює в інтернет-мережі, концентрується на інформаційних ресурсах та різних технічних пристроях в електронній формі, а їхня доступність надає можливість використовувати означений інформаційний пласт з метою протидії злочинності. Таким чином, вивчення та аналіз цих потужних інформаційних потоків набуває важливого значення у питанні криміналістичного забезпечення протидії злочинності і, безперечно, потребує належної уваги з боку дослідників. І хоча окремі практичні підрозділи правоохоронних органів (кіберполіція, кримінальна поліція тощо) вже мають певні успішні спроби використання технології OSINT у протидії злочинності (встановлення особи злочинця, отримання іншої корисної довідкової інформації), проте така діяльність не є системною, без залучення фахівців у певній галузі криміналістичних знань (наприклад спеціалістів з портретної та фототехнічної експертизи), що, у свою чергу, впливає на швидкість та оперативну доцільність прийняття важливих процесуальних рішень[1].

[1] До речі, розвідку на базі аналізу відкритих джерел інформації фахівці США ведуть з лютого 1941 року, коли в складі Комісії з комунікацій (Federal Communications Commission) була заснована Foreign Broadcast Monitoring Service (FBMS). Її головним завданням був контроль радіомовлення країн нацистського блоку, на її функціонування було виділено 150 тис. дол. [1].

З відкритих джерел ми дізнаємося, що OSINT (англ. Open source intelligence) – це концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення законів – для підтримки прийняття рішень у сфері національної оборони і безпеки. Вона включає в себе: пошук інформації, реєстрацію та облік інформації, аналіз інформації і синтез повідомлень з різних джерел, адміністрування та розповсюдження інформації. Специфічність такої інформації пов'язана з тим, що вона є результатом аналітичної обробки великого обсягу відкритого, загальнодоступного[2] інформаційного потоку, яким є: а) ЗМІ: друковані газети, журнали, радіо та телебачення; б) всесвітня мережа «Інтернет»: онлайн-публікації, блоги, дискусійні групи (форуми), медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube, RuTube та інші відеохостинги, вікі-довідники та інші вебсайти соціальних медіа (фейсбук, твітер, інстаграм, телеграм та ін.). Ці джерела також випереджають безліч інших джерел через своєчасність і легкість доступу; в) офіційні державні джерела: публічні урядові звіти, бюджети, слухання, телефонні довідники, пресконференції, вебсайти та виступи. Хоча ці джерела походять з офіційних джерел, вони є публічно доступними і можуть використовуватися відкрито і вільно; г) професійні та академічні публікації: інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дипломів та дисертацій; д) комерційні дані: комерційні зображення, фінансові та промислові оцінки, бази даних; е) інша література: технічні звіти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені [8; 9].

За таких підстав особливий криміналістичний інтерес становить технологія автоматичної ідентифікації особи людини за елементами зовнішності за її відображенням на фотографії або відеозаписі, яка має широке комерційне та наукове застосування. Дана технологія цікава тому, що може здійснюватися без контакту з об'єктом пошуку. У всесвітній мережі є онлайн-сервіси пошуку осіб за елементами зовнішності серед масиву фотозображень, що містяться у популярних соціальних мережах («Search4faces», «VK.watch» та ін.) на особистих сторінках осіб [10; 11]. За результатами пошуку сервіси надають користувачу масив, що складається з переліку максимально схожих осіб, із відсотковим зазначенням збігу зовнішності обличчя знайденої особи з досліджуваною. Тобто отримані результати не містять інформацію про індивідуально-конкретну тотожність осіб, оскільки до такого висновку можна дійти або шляхом суб'єктивної оцінки співпадаючих ознак зовнішності людини, або використовуючи спеціальні методи портретної експертизи. При цьому важливо розуміти, що візуальне сприйняття ознак зовнішності особами, які не є спеціалістами в галузі судово-портретної експертизи, ґрунтується лише на підставі суб'єктивної оцінки окремих ознак та внутрішнього переконання. І навпаки, спеціалісти оцінюють збіг зовнішності порівнюваних осіб, застосовуючи науково-обґрунтовані спеціальні методи портретної експертизи, що дає змогу об'єктивно проаналізувати результати пошуку.

[2] У рамках OSINT терміни «відкрите джерело» та «загальнодоступна інформація» використовуються у значеннях: а) відкрите джерело – особа або група осіб, які надають інформацію без вимоги збереження її конфіденційності – інформація або відносини, незахищені від публічного розкриття. Відкриті джерела належать до сфери загальнодоступної інформації і не мають обмеження в доступі для фізичних осіб; б) загальнодоступна інформація – дані, факти, інструкції або інші матеріали, опубліковані чи розміщені для широкого використання, які доступні для громадськості, законно побачені або почуті випадковими спостерігачами, представлені на відкритих зустрічах для громадськості [8].

Безпосереднє разове опробування на практиці технології OSINT відразу дозволило виявити її позитивні сторони, зокрема:

1) її використання не вимагає додаткових фінансових витрат на: а) придбання спеціальної техніки та програмного забезпечення, адже достатньо мати лише доступ до всесвітньої мережі «Інтернет» та робочу станцію ПК (смартфон, планшет); б) підготовку певних спеціалістів, оскільки технологія OSINT достатньо проста як в опануванні, так і в обробці вихідної та отриманні криміналістично значущої інформації;

2) вона є у вільному доступі, а тому може бути використана не лише суб'єктами правоохоронної діяльності (представниками державної влади), а й приватними детективами, волонтерами та ін.;

3) її використання (за певних умов) не порушує прав громадян.

З огляду на наведене вище та на підставі власної ініціативи було зроблено спробу практичної реалізації цієї технології з метою отримання криміналістично значущої інформації задля викриття злочинів[3]. Ми виходили з того, що фото/відеоконтент обставин скоєння злочину (підготовка, безпосередньо факт вчинення злочину та/або його приховування) оперативно розміщується їх авторами (інколи наввипередки) у популярних соціальних мережах (наприклад «Інстаграм», «Фейсбук» та ін.). Як згодом з'ясувалося, найбільш затребуваним у цьому плані серед інших виявився месенджер «Телеграм» – месенджер, програмне забезпечення якого дозволяє обмінюватися текстовими повідомленнями, графічними та відеофайлами, а також безкоштовно телефонувати іншим користувачам програми [9]. При цьому аналіз повідомлень засвідчив, що вони: 1) створюються: а) безпосередньо свідками певної події або потерпілими; б) у довільній формі; 2) містять текстовий меседж, до якого зазвичай додається файл з фото або відеозаписом з відображенням на них: а) осіб, що їх вчинили; б) механізму (способу) вчинення; в) транспортних засобів, які були задіяні та г) інших обставин, які мають значення для розкриття та розслідування кримінальних правопорушень; 3) хронологічно розміщуються у стрічці новин відповідних тематичних пабліків (наприклад, «Київ Оперативний», «Дніпро Оперативний / Днепр Оперативный», «Харків Оперативний / Харьков Оперативный», «Треш Харків / Треш Харьков» тощо) (див. рис. 5–7); 4) містять не лише інформацію про кримінальні або адміністративні правопорушення, але й іншу інформацію (про зниклих осіб та інше).

[3] Додатковою мотивацією у цьому питанні стали перераховані нижче обставини. У 1911 р. відомий російський художник-графік Валентин Олександрович Сєров написав (намалював, створив) картину під назвою «Портрет невідомої». Припущень про особу зображеної було багато, але всі вони залишалися просто припущеннями, поки на виставці в музеї цю картину не побачив київський художник Веніамін Васильович Ларін. На згаданій картині погляд художника вловив знайомі риси обличчя – актриси Олександри Олександрівни Яблочкіної. Підготувавши всі необхідні порівняльні матеріали, зацікавлені особи звернулися до спеціалістів Державного науково-дослідного експертно-криміналістичного центру МВС України з проханням проведення портретного дослідження, метою якого було встановити, чи одна і та ж особа зображена на графічному портреті Валентина Сєрова та фотознімках актриси Олександри Яблочкіної (див. рис. 14, 15). І хоча для київських криміналістів це був перший досвід роботи з художніми творами, вони професійно з цим упоралися. У висновку було зазначено, що за винятком більш темного відтінку очей на кольоровій фотографії актриси в порівнянні з малюнком Сєрова та контуру брів, усі інші антропометричні ознаки збіглися: пропорційне співвідношення висоти і ширини обличчя, форма і контур шиї, лінія росту волосся, будова й посадка очей, форма і контур носа, носогубні западини, контури підборіддя і рота [16].

Безпосередньо сам процес пошуку осіб за ознаками зовнішності із застосуванням згадуваної технології умовно можна поділити на чотири етапи.

Етап № 1 (курсив наш. – *Прим. авт.*). Моніторинг та аналіз змісту відео- і фотозображень та текстових повідомлень, що містяться у відкритому доступі на платформах різних інтернет-видань, відеохостингів, месенджерів та соціальних мереж. Мета – визначення наявності в них невстановлених осіб, зображення облич яких за комплексом відображених ознак утворюють сукупність, необхідну для ідентифікації за ознаками зовнішності. Так, 14.06.2020 року в тематичній групі «Київ Оперативний / Kyiv Operative», у якій висвітлюються оперативні новини про ДТП та кримінальну хроніку в місті Києві та Київській області, у месенджері «Телеграм» (https://t.me/s/KyivOperativ) було розміщено повідомлення щодо факту вчинення шахрайських дій (див. рис. 1). На одному з доданих до повідомлення фотозображень містилося зображення обличчя особи-правопорушника, особисті дані якого необхідно було встановити. Після опрацювання спеціалістом у галузі портретної експертизи згадуваного фотозображення обличчя особи-правопорушника, останнє було визнане придатним для подальшої ідентифікації за ознаками зовнішності.

Етап № 2 (курсив наш. – *Прим. авт.*). Використання загальнодоступних онлайн-сервісів автоматизованого пошуку осіб зі збіжними ознаками зовнішності серед масиву фотозображень, добровільно розміщених на серверах соціальних мереж «Вконтакті», «Одноклассники» та ін. За результатами такого пошуку сервіси соціальних мереж видають масиви фотозображень схожих осіб, визначаючи їх ступінь збігу у відсотковому значенні (див. рис. 2).

Етап № 3 (курсив наш. – *Прим. авт.*). Оцінка результатів пошуку із застосуванням спеціальних методів дослідження, що використовуються у галузі судової портретної експертизи. Так, до спеціальних методів можна віднести такі: а) метод зіставлення (візуальне, із застосуванням «масок», за допомогою накладання координатної сітки, відносних величин, на біологічну асиметрію, за допомогою аплікацій); б) методи суміщення зображень по медіальній та ламаній лініях; в) методи накладання (накладання-додавання, додавання-віднімання) [14]. Звичайно, провідна роль на даному етапі належить спеціалісту, що має кваліфікацію судового експерта за експертною спеціальністю 6.2 «Ідентифікація особи за ознаками зовнішності за матеріальними зображеннями». Його завдання полягає в тому, щоб на підставі науково обґрунтованої методики сформувати позитивний або негативний висновок про тотожність порівнюваних осіб та наочно це проілюструвати, *для запобігання виникненню сумнівів* (див. рис. 3) (курсив наш. – *Прим. авт.*).

Етап № 4 (курсив наш. – *Прим. авт.*). Аналіз змісту соціальних сторінок. Наявний практичний досвід продемонстрував, що соціальні сторінки (у більшості випадків) містять *обмежену* інформацію, де зазвичай відображається: а) прізвище та ім’я (без зазначення ім’я по батькові); б) число, місяць та рік народження; в) коло друзів; г) місце проживання (лише із зазначенням населеного пункту); д) місце навчання або роботи тощо. До того ж ці дані можуть виявитися *повністю або частково* «фейковими» (такими, що не відповідають дійсності). З огляду на наведене вище, на заключному четвертому етапі шляхом вивчення змісту соціальної сторінки (посилання на яку отримане на попередніх етапах), а також збору, об’єднання (зіставлення) та аналізу даних з основних публічних реєстрів і баз даних України [12], інформація про розшукувану особу *актуалізується та доповнюється* (див. рис. 4) (курсив наш. – *Прим. авт.*).

Саме за таким алгоритмом, використовуючи технологію OSINT, спеціалісти судово-портретної експертизи Харківського науково-дослідного експертно-криміналістичного

центру МВС України в період з жовтня 2019 року й до лютого 2020 року включно ідентифікували 22 особи (з понад 95 досліджених матеріалів)[4], серед яких були особи, які: а) вчинили кримінальні правопорушення як проти життя і здоров'я (вбивства, нанесення тілесних ушкоджень тощо), так і майнового характеру (крадіжки, грабежі, розбої тощо) (див. рис. 8, 9); б) брали участь у масових скупченнях людей (стихійні мітинги, футбольні матчі, акції протесту); в) беруть або брали участь у незаконних збройних формуваннях на тимчасово окупованих територіях Донецької, Луганської областей та Автономної Республіки Крим (див. рис. 10, 11); г) використовували платформи інтернет-видань, сайтів, відеохостингів для ведення антидержавної агітації та пропаганди, закликів до повалення державного устрою (див. рис. 12, 13). До того ж згадувані технології дозволяють встановити як особисті зв'язки розшукуваних осіб, які переховуються від правоохоронних органів (близькі родичі, друзі, знайомі тощо), так і місця їхнього фактичного перебування.

Тобто ефективність запропонованої моделі використання технології автоматичної ідентифікації особи людини за елементами зовнішності за її відображенням на фотографії або відеозаписі – беззаперечна (і це за відсутності матеріальних витрат). Водночас залишається відкритим питання формату реалізації інформації, отриманої в результаті OSINT-пошуку. Щодо цього заслуговує на увагу позиція практиків, які пропонують оформлювати результати OSINT-пошуку у вигляді письмової консультації спеціаліста, де останній *у вірогідній формі* надає *орієнтуючу інформацію* про невпізнану особу (правопорушника, свідка, потерпілого тощо) та інші відомості, що мають суттєве значення для встановлення її фактичного місцезнаходження (склад сім'ї, місце реєстрації, судові рішення та інше) [17] (курсив наш. – *Прим. авт.*).

Звичайно, отримана в ході моніторингу соціальних мереж інформація може бути використана й у процесі розслідування кримінальних проваджень, у рамках яких для вирішення завдань з ідентифікації особи за ознаками зовнішності будуть призначені відповідні експертизи (наприклад, для встановлення фактів внесення редакторських змін у вигляді монтажу в цифрових фотозображеннях доцільно призначити комплексну судово-портретну та судово-фототехнічну експертизи) [15].

Висновки. Таким чином, з огляду на наведене вище та з метою підвищення ефективності використання технології OSINT у протидії злочинності можна пропонувати створення міжвідомчих аналітично-пошукових груп (а можливо, й підрозділів) у системі органів внутрішніх справ. Як варіант можна розглядати гармонійне поєднання професійних можливостей фахівців фототехнічних та портретних видів досліджень Експертної служби МВС України та працівників окремих підрозділів поліції (Департаменту кіберполіції Національної поліції України), що створить передумови для оперативного та якісного дослідження криміналістично значущої інформації, яка міститься у відкритих джерелах інтернет-ресурсів.

[4] Вивчалися фото та відеоматеріали з зображенням невідомих осіб, що були причетними до вчинення правопорушень на території Харківської та Київської областей. Джерелом такої інформації стали відкриті повідомлення у стрічках новин тематичних груп, створених у месенджері «Телеграм», а саме: «Київ Оперативний / Kyiv Operative», «Типовий Харків / Типичный Харьков», «Харків 1654 / Харьков 1654», «Харків Live / Харьков Live», «СонцеЛикий Харків / СолнцеЛикий Харьков», «Треш Харків / Трэш Харьков», «Типове ХТЗ / Типичное ХТЗ», «Харків Оперативний / Харьков Оперативный», «True.Ха» та ін.

Додатки

Рис. 1. Аналіз змісту фотозображень та повідомлення, що містяться у відкритому доступі у групі «Київ Оперативний» месенджера «Телеграм», на яких зафіксовані обставини події за фактом вчинення шахрайських дій

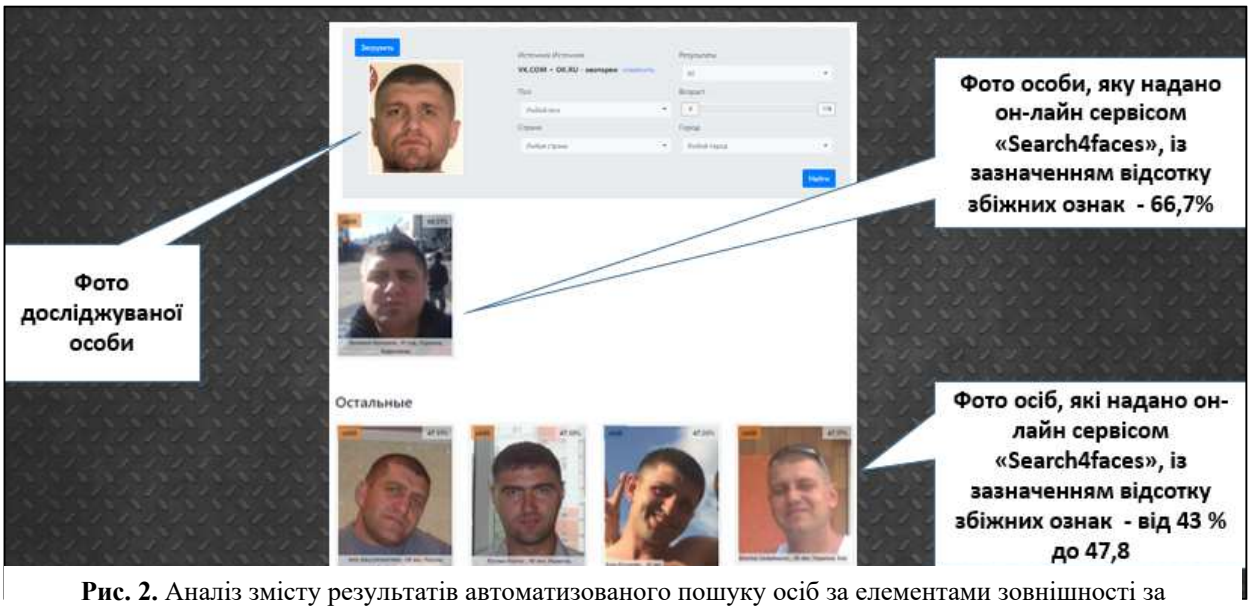


Рис. 2. Аналіз змісту результатів автоматизованого пошуку осіб за елементами зовнішності за допомогою онлайн-сервісу «Search4faces» (https://search4faces.com) серед масиву фотозображень у соціальних мережах «Вконтакті» та «Одноклассники»

Рис. 3. Порівняльне дослідження зовнішності осіб із застосуванням методів портретної експертизи досліджуваної особи (Особа-1) та наданої за результатом пошуку онлайн-сервісу «Search4faces» (https://search4faces.com) (Особа-2)

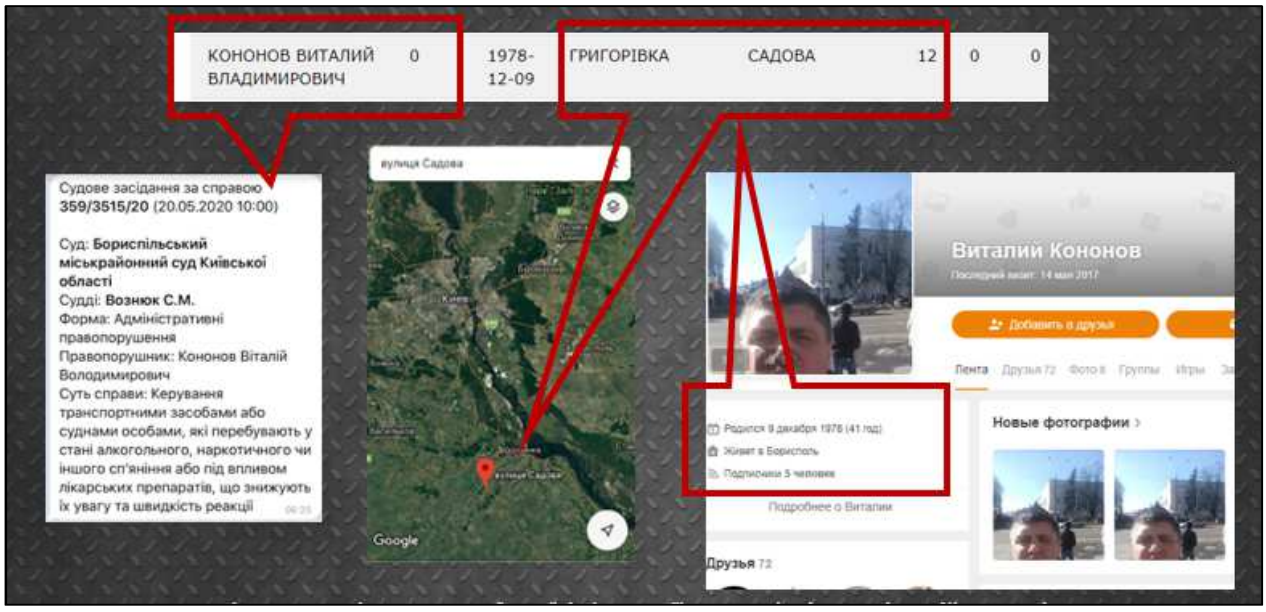


Рис. 4. Аналітичне дослідження особистої інформації на сторінці в соціальній мережі «Однокласники», інформаційного інтернет-ресурсу «Вся Україна» (http://nomer-org.space/allukraina/), а також даних, отриманих за запитом у телеграм-боті «Open Data Bot»

.

Рис. 5–7. Зразки повідомлень із медійним змістом про факти вчинення правопорушень, які розміщені в тематичних групах («Типовий Харків / Типичный Харьков», «Харків Live / Харьков Live») у месенджері «Телеграм»

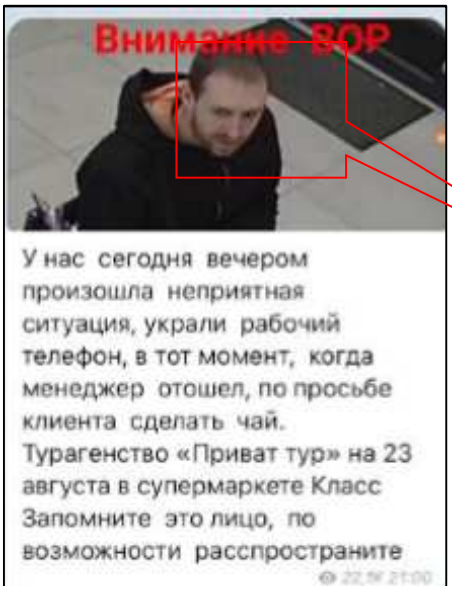


Рис. 8. Повідомлення в групі «Харків 1654 / Харьков 1654» в месенджері «Телеграм» про те, що зображена на ілюстрації невідома особа здійснила крадіжку телефона

Рис. 9. Зображення схожої за ознаками зовнішності особи на сторінці соціальної мережі «Ok.ru»

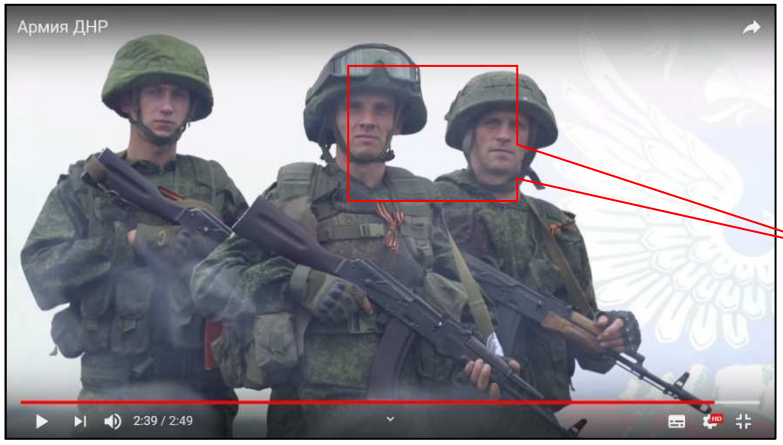


Рис. 10. Кадр, зроблений о 00:02:39, з відеозапису «Армія ДНР», що розміщений на платформі відеохостингу «Youtube.com» із зображенням трьох осіб

Рис. 11. Зображення схожої за ознаками зовнішності особи на сторінці соціальної мережі «Vk.com»

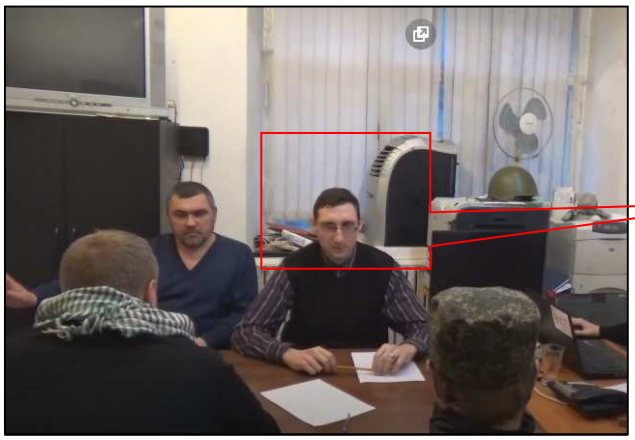


Рис. 12. Кадр, зроблений о 00:01:22, з відеозапису «ХНР. Засідання і резолюція Комітету 27», що розміщений на платформі відеохостингу «Youtube.com» із зображенням невідомих осіб

Рис. 13. Зображення схожої за ознаками зовнішності особи на сторінці соціальної мережі «Vk.com»

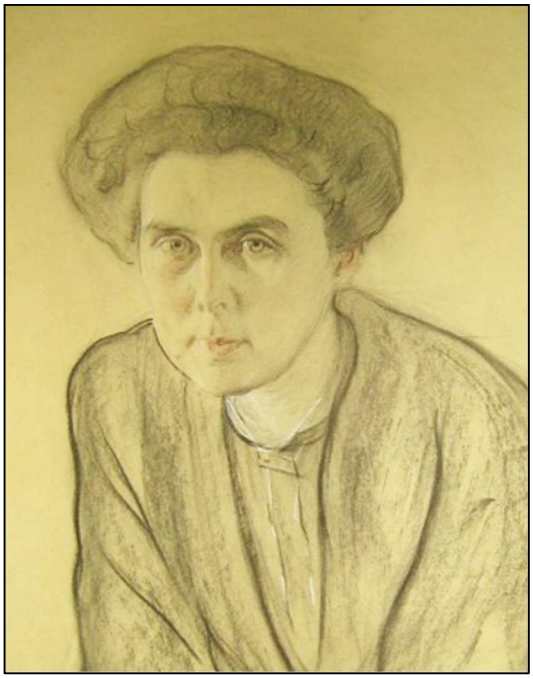


Рис. 14. В. О. Сєров «Портрет невідомої», 1911 рік

Рис. 15. Фотозображення актриси О. О. Яблочкіної

Список використаних джерел

1. Кожушко О. О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: http://jrnl.nau.edu.ua/index.php/IMV/ article/viewFile/3264/3217 (дата звернення: 11.05.2020).
2. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв'язку.* 2016. Вип. 4. С. 81–84. URL: http://nbuv.gov.ua/UJRN/suntz_2016_4_22 (дата звернення: 05.06.2020).
3. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Применение OSINT в аналитической деятельности. *Реєстрація, зберігання і обробка даних :* збірник матеріалів щорічної підсумкової наукової конференції (м. Київ, 17–18 травня 2018 року). Київ: ІПРІ НАН України, 2018. С. 110–112.
4. Жарков Я. М., Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Військово-спеціальні науки»*. 2013. Вип. 30. С. 38–41. URL: http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12 (дата звернення: 07.06.2020).
5. Bellingcat. URL: https://www.bellingcat.com (дата звернення: 07.06.2020).
6. The MH17 Trial Part 1: New Material From The Four Defendants. URL: https://www.bellingcat.com/news/uk-and-europe/2020/04/20/the-mh17-trial-part-1-new-materials-from-the-four-defendants (дата звернення: 08.06.2020).
7. Центр Миротворець. URL: https://myrotvorets.center (дата звернення: 08.06.2020).
8. Open-source intelligence (OSINT). Електронна енциклопедія Wikipedia. URL: http://en.wikipedia.org/wiki/Open-source_intelligence (дата звернення: 10.06.2020).
9. Telegram. Електронна енциклопедія «Вікіпедія». URL: https://uk.wikipedia.org/wiki/Telegram (дата звернення: 10.06.2020).
10. Онлайн-сервис поиска людей по фотоизображению «Search4faces». URL: https://search4faces.com (дата звернення: 02.03.2020).
11. Онлайн-сервис поиска людей по фотоизображению «Vk.watch». URL: https://vk.watch (дата звернення: 02.03.2020).
12. Перелік відкритих реєстрів та баз даних України. URL: https://investment.zoda.gov.ua/uk/perelik-vidkritih-restriv-ta-baz-danih-ukraini (дата звернення: 22.07.2020).
13. Кримінально-процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 25.07.2020).

14. Коструб А. М., Павленко О. С., Чашницька Т. Г. Методика ідентифікації особи за ознаками зовнішності за матеріальними зображеннями. К.: ДНДЕКЦ МВС України, 2013. 31 с.

15. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08 жовтня 1998 року № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 25.07.2020).

16. Шпетная А. Опознание неизвестной на портрете Серова с помощью криминалистики. URL: https://shakko-kitsune.livejournal.com/1226728.html (дата звернення: 25.07.2020).

17. Шевцов С. О., Кожевніков О. А. Консультації спеціаліста на стадії досудового розслідування : практ. посібник / М-во внутр. справ України; Експертна служба; Харківський наук.-дослід. експерт.-криміналіст. центр. Харків, 2020. 43 с.

18. Шепітько В. Ю. Роль сучасних інформаційних технологій у встановленні особи злочинця. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. Харків, 2014. Вип. 14. С. 5–11.

19. Панасюк А. О. Алгоритмізація використання мережі Інтернет при виявленні та розслідуванні злочинів. *Правова держава*. 2019. № 34. С. 95–100.

References

1. Kozhushko, O. O. (2011). Rozvidka vidkrytykh dzherel informatsii (OSINT) u rozviduvalnii praktytsi SShA [Open Source Intelligence (OSINT) in US intelligence practice]. URL: http://jrnl.nau.edu.ua/index.php/IMV/ article/viewFile/3264/3217 (data zvernennia: 11.05.2020) [in Ukrainian].

2. Mynko, O. V., Iokhov, O. Yu., Olenchenko, V. T., Vlasov, K. V. (2016). Vykorystannia tekhnolohii OSINT dlia otrymannia rozviduvalnoi informatsii [Using OSINT technology to obtain intelligence]. *Systemy upravlinnia, navihatsii ta zviazku.*Vyp. 4. S. 81–84. URL: http://nbuv.gov.ua/UJRN/suntz_2016_4_22 (data zvernennia: 05.06.2020) [in Ukrainian].

3. Dodonov, A. G., Lande, D. V., Putyatin, V. G. (2018). Primenenie OSINT v analiticheskoj deyatel'nosti [Applying OSINT to Analytics]. Reiestratsiia, zberihannia i obrobka danykh : zbirnyk mat. shchorichnoi pidsumkovoi naukovoi konferentsii (m. Kyiv 17–18 travnia 2018 roku. Kyiv: IPRI NAN Ukrainy. S. 110–112 [in Russian].

4. Zharkov, Ya. M., Vasyliev, A. O. (2013). Naukovi pidkhody shchodo vyznachennia suti rozvidky z vidkrytykh dzherel [Scientific approaches to determining the nature of intelligence from open sources]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka.*Vyp. 30. S. 31–41. URL: http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12 [in Ukrainian].

5. Bellingcat. URL: https://www.bellingcat.com.

6. The MH17 Trial Part 1: New Material From The Four Defendants. URL: https://www.bellingcat.com/news/uk-and-europe/2020/04/20/the-mh17-trial-part-1-new-materials-from-the-four-defendants (data zvernennia: 08.06.2020).

7. Tsentr Myrotvorets [Peacemaker Center]. URL: https://myrotvorets.center (data zvernennia: 08.06.2020) [in Ukrainian].

8. Open source intelligence (OSINT). URL: http://en.wikipedia.org/wiki/Open-source_intelligence (data zvernennia: 10.06.2020).

9. Telegram. URL: https://uk.wikipedia.org/wiki/Telegram (data zvernennia: 10.06.2020).

10. Onlajn-servis poiska lyudej po fotozobrazhennyu «Search4faces». [Search4faces online service for searching people by photo]. URL: https://search4faces.com (data zvernennia: 02.03.2020) [in Russian].

11. On-lajn servis poiska lyudej po fotozobrazhennyu «Vk.watch». [Vk.watch online service for searching people by photo]. URL: https://vk.watch (data zvernennia: 02.03.2020) [in Russian].

12. Perelik vidkrytykh reiestriv ta baz danykh Ukrainy [The list of open registers and databases of Ukraine]. URL: https://investment.zoda.gov.ua/uk/perelik-vidkritih-restriv-ta-baz-danih-ukraini (дата звернення: 22.07.2020) [in Ukrainian].

13. Kryminalno-protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (data zvernennia: 25.07.2020) [in Ukrainian].

14. Kostrub, A. M., Pavlenko, O. S., Chashnytska, T. H. (2013). Metodyka identyfikatsii osoby za oznakamy zovnishnosti za materialnymy zobrazhenniamy [Methods of identification of a person on the basis of appearance by material images]. K.: DNDEKTs MVS Ukrainy. 31 s. [in Ukrainian].

15. Pro zatverdzhennia Instruktsii pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen ta Naukovo-metodychnykh rekomendatsii z pytan pidhotovky ta pryznachennia sudovykh ekspertyz ta ekspertnykh doslidzhen [About approval of the Instruction on appointment and carrying out of forensic examinations and expert researches and Scientific and methodical recommendations concerning preparation and appointment of forensic examinations and expert researches] : nakaz Ministerstva yustytsii Ukrainy vid 08 zhovtnia 1998 roku № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (data zvernennia: 25.07.2020) [in Ukrainian].

16. SHpetnaya A. (2018). Opoznanie neizvestnoj na portrete Serova s pomoshch'yu kriminalistiki [Identification of the unknown in Serov's portrait using forensic science]. URL: https://shakko-kitsune.livejournal.com/1226728.html (data zvernennia: 25.07.2020) [in Russian].

17. Shevtsov, S. O., Kozhevnikov, O. A. (2020). Konsultatsii spetsialista na stadii dosudovoho rozsliduvannia [Consultations of a specialist at the stage of pre-trial investigation] : prakt. posibnyk / M-vo vnutr. sprav Ukrainy; Ekspertna sluzhba; Kharkivskyi nauk.-doslid. ekspert.-kryminalist. tsentr. Kharkiv. 43 s. [in Ukrainian].

18. Shepitko, V. Yu. (2014). Rol suchasnykh informatsiinykh tekhnolohii u vstanovlenni osoby zlochyntsia [The role of modern information technology in establishing the identity of the offender]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky* : zb. nauk. pr. Kharkiv. Vyp. 14. S. 5–11 [in Ukrainian].

19. Panasiuk, A. O. (2019). Alhorytmizatsiia vykorystannia merezhi Internet pry vyiavlenni ta rozsliduvanni zlochyniv [Algorithmization of the use of the Internet in the detection and investigation of crimes]. *Pravova derzhava*. № 34. S. 95–100 [in Ukrainian].

Oderiy Oleksiy,
Doctor in Law, Associate Professor
(Donetsk Law Institute, MIA of Ukraine, Mariupol)
ORCID: https://orcid.org/0000-0002-6999-4387

Kozhevnikov Oleksiy,
Aspirant
(Kharkiv National University of Internal Affairs, MIA of Ukraine, Kharkiv)
ORCID: https://orcid.org/0000-0001-8976-0863

GETTING CRIMINALLY SIGNIFICANT BY ANALYSIS OF OPEN INTERNET SOURCES

The article considers OSINT (Open source intelligence) technology, which is intelligence based on open sources. Development of digital means of photo and video recording, led to the emergence of a large number of media files that reproduce the objective situation at different intervals of time and space. Based on the analysis, it is proved that Open source intelligence can be successfully used by law enforcement agencies to solve specific forensic problems. Its advantages are identified, which are as follows: 1) its use does not require additional financial costs for: a) purchase of special equipment and software, because it is enough to have access to the World Wide Web and PC workstation (smartphone, tablet); b) training of certain specialists, as OSINT technology is quite simple both in mastering and in processing the source and obtaining forensic information; 2) it is freely available, and therefore can be used not only by law enforcement agencies (government officials), but also by private detectives, volunteers, etc.; 3) its use (under certain conditions) does not violate the rights of citizens. Practical examples of application of online services on search of the persons fixed on a photo or video images on anthropometric data are resulted. There are four main stages of the process of searching for people by appearance on the mentioned technology. It was stated that using OSINT technology, forensic experts of the Kharkiv Research Forensic Center of the Ministry of Internal Affairs of Ukraine in the period from October 2019 to February 2020 identified 22 people (from more than 95 researched materials), evidence in criminal proceedings. Of course, the information obtained during the monitoring of social networks can be used in the investigation of criminal proceedings, in which to solve the problem of identifying a person by appearance, appropriate examinations will be appointed. It is proposed to create interdepartmental analytical and search groups m the system of bodies of the Ministry of Internal Affairs of Ukraine.

Key words: *OSINT; Face ID; social media; social networking; Instagram; Facebook; Telegram; VK; Face Forensics.*

Надійшла до редколегії 15.09.2020