DOI https://doi.org/10.30525/2592-8813-2021-3-10

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КІБЕРРОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ ЯК МЕТОДУ ОТРИМАННЯ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ

Олена Козицька,
доцент кафедри кримінального права та процесу
Хмельницького університету управління та права
імені Леоніда Юзькова (Хмельницький, Україна)
ORCID ID: 0000-0002-3045-8181
o.kozytska@ukr.net

Анотація. Стаття присвячена дослідженню кіберрозвідки на основі відкритих джерел як методу отримання криміналістично значущої інформації задля виконання завдань, спрямованих на виявлення, розкриття та розслідування кримінальних правопорушень, встановлення місцезнаходження розшукуваних осіб. Під час написання статті використовувалися діалектико-матеріалістичний метод наукового пізнання, формально-логічний, історико-правовий, порівняльно-правовий, системний метод, а також методи аналізу та синтезу. Проаналізовано погляди науковців щодо визначення розвідки на основі відкритих джерел (OSINT), охарактеризовані різні види інформації, запропоновано класифікацію джерел відкритої інформації, розміщеної в кіберпросторі. Зазначено основні категорії криміналістично значущої інформації, які можна отримати в результаті розвідки в кіберпросторі. Визначено та досліджено такі етапи кіберрозвідки на основі відкритих джерел, як визначення мети і завдань кіберрозвідки, планування, пошук, збирання та обробка інформації, отриманої з відкритих джерел, її аналіз та оцінка, формування висновків та підготовка результатів.

Ключові слова: інформація, кіберрозвідка, OSINT, криміналістично значуща інформація, відкрите джерело інформації, пошук інформації, розслідування кримінальних правопорушень.

GENERAL CHARACTERISTICS OF OPEN-SOURCE CYBERINTELLIGENCE AS A METHOD OF OBTAINING FORENSICALLY RELEVANT INFORMATION

Olena Kozytska,
Ph.D. in Law,
Associate Professor at the Department of Criminal Law and Procedure
Leonid Uzkov Khmelnytskyi University of Management and Law (Khmelnytskyi, Ukraine)
ORCID ID: 0000-0002-3045-8181
o.kozytska@ukr.net

Abstract. The article is devoted to the study of open-source cyberintelligence as a method of obtaining criminally relevant information to perform tasks aimed at the detection, disclosure and investigation of criminal offences, the establishment of the location of wanted persons. When writing the article was used dialectical-materialistic method of scientific knowledge, formal-logical, historical-legal, comparative-legal, systematic method, as well as methods of analysis and synthesis. The author analyses scientists' views on the definition of open source intelligence (OSINT), characterizes different types of information, proposes a classification of sources of open information placed in cyberspace. The main categories of criminally relevant information that can be obtained as a result of intelligence in cyberspace are specified. The following stages of cyberintelligence based on open source were identified and investigated: defining the purpose and objectives of cyberintelligence; planning; search, collection and processing of information obtained from open sources; its analysis and evaluation; drawing of conclusions and preparation of results.

Key words: information, cyber-intelligence, OSINT, forensically relevant information, open source information, information retrieval, criminal investigation.

Вступ. У 1815 році німецький банкір Натан Ротшильд зазначив: «Хто володіє інформацією, той володіє світом». Ця фраза одразу стала афоризмом, а з роками набула ще більшої актуальності. Дійсно, невпинне зростання обсягів різноманітної інформації, експоненціальне збільшення «великих даних» перетворило оброблену та належним чином структуровану інформацію на один із найбільш дорогоцінних ресурсів людства, здобуття якого залишається пріоритетним напрямом розвідувальної діяльності різноманітних служб. Звісно, якісне виконання завдань, спрямованих на профілактику, виявлення, розкриття та розслідування кримінальних правопорушень, також є неможливим без своєчасного отримання актуальної криміналістичної значущої інформації з різних джерел, у тому числі і тих, які знаходяться у відкритому доступі.

Стан наукових досліджень. Практику використання можливостей розвідки на основі відкритих джерел було впроваджено ще на початку 40-х років минулого століття розвідувальним співтовариством США (Williams & Blum, 2018: 4), і відтоді тривають наукові дослідження вказаного методу здобуття інформації. Значний внесок у вивчення цієї проблематики зробили такі зарубіжні дослідники, як S. Adams, C. Altheide, M. Bazzell, A. Bielska, H. Carvey, N.A. Hassan, S.D. Gibson, R. Hijazi, J. Selianko, R.D. Steele тощо. Водночас українські вчені не залишили поза увагою зазначену тему. Особливостям розвідки на основі відкритих джерел присвятили свої праці С.В. Албул, О.М. Бандурка, В.В. Бурба, Р.О. Гончар, М.Л. Грібов, К.Ю. Ісмайлов, О.О. Кожушко, С.С. Мирза, Д.Й. Никифорчук, М.А. Погорецький, І.А. Федчак та багато інших.

Водночас окремі аспекти використання методу розвідки на основі відкритих джерел у процесі виявлення, розкриття та розслідування кримінальних правопорушень залишаються мало висвітленими. Також потребують більш детального дослідження особливості розвідки на основі саме тих відкритих джерел, котрі розміщені в кіберпросторі (так званої кіберрозвідки на основі відкритих джерел), адже у зв'язку з інформаційно-технічним прогресом людства значний обсяг інформації зберігається в цифровому вигляді та утворює масив «великих даних».

Метою нашої статті є дослідження особливостей кіберрозвідки на основі відкритих джерел як методу отримання криміналістично значущої інформації задля виконання завдань, спрямованих на виявлення, розкриття та розслідування кримінальних правопорушень.

Методи дослідження. Під час написання статті застосовувалася низка загальнонаукових та спеціальних методів наукового пізнання. Зокрема, історико-правовий метод використовувався в процесі вивчення наукових праць, присвячених розвідці на основі відкритих джерел, порівняльно-правовий – під час аналізу поглядів вчених щодо досліджуваних наукових категорій, визначень та підходів, системний – у процесі побудови класифікації відкритих джерел інформації в кіберпросторі. Також широко застосовувалися діалектико-матеріалістичний метод наукового пізнання соціально-правових явищ, формально-логічний метод, а також методи аналізу та синтезу.

Виклад основного матеріалу. Насамперед зазначимо, що поняття «розвідка на основі відкритих джерел» у науковій літературі зазвичай позначається англомовним акронімом OSINT (англ Open Source Intelligence – розвідка на основі відкритих джерел). Незважаючи на те, що протягом століть відбувався збір розвідувальної інформації шляхом використання загальнодоступних ресурсів, конкретна дата, коли було запроваджено вживання терміна OSINT, відсутня (Hassan & Hijazi, 2018: 1).

Нині під OSINT розуміють:

– один із напрямів розвідки, який включає пошук, вибір та збирання розвідувальної інформації, отриманої із загальнодоступних джерел, а також її аналіз (Dodonov et al., 2017: 62);

– збирання із загальнодоступних джерел (засобів масової інформації, соціальних мереж, форумів і блогів тощо), оцінку, аналіз та поширення інформації про особу, подію чи загрозу з розвідувальною метою або з метою використання її як доказу під час проведення розслідувань (Adams, 2020);

– технологію «глибинного збирання» різнорівневої різноформатної інформації, а також створення на її основі принципово нових знань з їх подальшою візуалізацією (Ataian, Gureva & Sharabaeva, 2021: 13).

Концепція OSINT базується на двох основних поняттях:

а) відкрите джерело інформації – це джерело, що надає інформацію без вимоги збереження конфіденційності. Відкриті джерела належать до середовища загальнодоступної інформації, тобто будь-які обмеження для фізичних осіб не встановлюються;

б) загальнодоступна інформація – це інформація, оприлюднена чи розміщена для широкого використання, доступна для громадськості (Dodonov et al., 2017: 62).

Однак перед тим, як більш детально розглядати джерела відкритої інформації, зосередимось на законодавчому та науковому визначеннях інформації, а також на окремих її видах.

Так, інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Це можуть бути інформація про фізичну особу, інформація довідково-енциклопедичного характеру, інформація про стан довкілля (екологічна інформація), інформація про товар (роботу, послугу), науково-технічна інформація, податкова інформація, правова інформація, статистична інформація, соціологічна інформація та інші види інформації (Zakon Ukrainy, 1992, No. 2657-XII).

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (конфіденційну, таємну та службову інформацію) (Zakon Ukrainy, 1992, No. 2657-XII).

Крім того, окремо можна виділити публічну інформацію, під якою розуміється відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом України «Про доступ до публічної інформації». Доступ до публічної інформації забезпечується шляхом систематичного та оперативного оприлюднення інформації в офіційних друкованих виданнях, на офіційних вебсайтах в мережі Інтернет, на єдиному державному вебпорталі відкритих даних, на інформаційних стендах, у будь-який інший спосіб, а також шляхом надання інформації за запитами на інформацію (Zakon Ukrainy, 2011, No. 2939-VI).

Публічна інформація також може існувати у формі відкритих даних, тобто у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення. Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації. Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному вебпорталі відкритих даних та на своїх вебсайтах (Zakon Ukrainy, 2011, No. 2939-VI).

У тлумачному словнику українських термінів зазначається, що інформація з відкритих джерел – це інформація, яка призначена для громадськості; інформація із зовнішніх джерел, наприклад, таких, як наукова література; офіційна інформація; інформація, що видається громадськими організаціями, комерційними компаніями і засобами масової інформації (Tlumachnyi slovnyk ukrainskykh terminiv, 2004, p. 13).

Інформація з відкритих джерел – це загальна поширена інформація, яка включає в себе дані, що можуть бути систематизовані за допомогою редакційного процесу, котрий забезпечує їх фільтрацію та перевірку (Selianko, 2001: 2).

На думку І.А. Федчака, під поняттям «інформація з відкритих джерел» (у контексті кримінального аналізу) слід розуміти окремі дані, записи, відомості, звіти, оцінки тощо, які мають значення для діяльності правоохоронних органів, не потребують дотримання юридичних вимог або застосування будь-якого типу негласних методів для їх збору та одержання (Fedchak, 2021: 144).

До відкритих джерел інформації зараховують:

– друковані (газети, часописи) і аудіовізуальні (радіо, телебачення) засоби масової інформації; книги, довідники, керівництва з експлуатації, інструкції з використання; наукові публікації; публічні звіти державних органів і виступи офіційних осіб; Інтернет (сторінки соціальних мереж, відеохостингів, блогів, форумів, електронних довідників), дані дистанційного зондування землі, аерофото- і супутникової зйомки (наприклад, Google Earth) тощо (Bilous, 2015: 32);

– засоби масової інформації (газети, журнали, радіо, телебачення та комп'ютерну інформацію); користувацький контент (соціальні мережі, сайти для зберігання відео, блоги; форуми, соціальні мережі, блоги, відеохостинги чи спільноти); загальнодоступні дані (інформацію про бюджет, демографічну ситуацію, пресконференції); міжнародні супутникові геосистеми; професійні та академічні праці (конференції, професійні асоціації, наукові роботи) (Shishliakov, 2017: 109);

– офіційні джерела; неофіційні відкриті джерела; засоби масової інформації; оголошення; рекламу; бази даних; висновки експертів; результати аналізу або спеціального оброблення даних, текстів за прямими або непрямими ознаками (Honchar, 2012: 69);

– традиційні засоби масової інформації (радіо, телебачення, друковані засоби масової інформації – газети, журнали, електронні засоби масової інформації, комерційний онлайн-контент); «сіру» літературу (академічні дослідження, конференції, виставки, експозиції, конгреси, зустрічі, статистичні дані та бази даних державних реєстрів та приватного сектора, дослідження ринку); комерційний продукт (спеціалізовані техніко-тактичні огляди, комерційні зображення, дані картографування, дослідження ринків); людей-свідків (сторонніх спостерігачів, експертів, бізнесменів, журналістів, мандрівників, науковців, біженців) (Gibson, 2007: 80).

Своєю чергою автори книги «Розпізнавання інформаційних операцій» розподіляють відкриті джерела інформації на дві категорії: основні та додаткові (похідні). На їхню думку, основним джерелом є документ або фізичний об'єкт, що містить інформацію, яка була написана чи створена за результатами проведених досліджень та їх аналізу. Як правило, така інформація є фрагментарною, неоднозначною та складною для аналізу. Це оригінали документів, виписки з них, переклади, наукові журнали, виступи, листи, інтерв'ю, новини, офіційні звіти, творчі роботи (поезія, драматургія, романи, музика та ін.), артефакти (кераміка, меблі, одежа, історичні будівлі тощо), розповіді та спогади людей. До додаткових або похідних джерел належать матеріали, підготовлені урядовими прес-службами, комерційними та неурядовими організаціями, прессекретарями (Dodonov et al., 2017: 72).

Ми вважаємо, що вказану класифікацію слід дещо доповнити і розподілити джерела відкритої інформації таким чином:

а) за формою існування: матеріальні (друковані газети, книги, записки, листи і т.п.); ідеальні (розповіді та спогади людей, лекції, інтерв'ю); електронно-цифрові (збережені на електронно-цифрових носіях інформації, розміщені в різних сегментах мережі Інтернет тощо). При цьому варто наголосити, що усі без винятку електронно-цифрові джерела інформації існують у кіберпросторі. Саме вони є предметом нашого дослідження, і надалі основна увага буде зосереджена лише на їх дослідженні, хоча ми цілком погоджуємося з Т.С. Яровим, який зазначає, що «у вільному доступі перебуває величезна кількість джерел інформації, і обмежувати їх коло виключно кіберпростором означає розглядати лише одну нішу OSINT» (Yarovoi, 2019: 203);

б) за способом подання інформації: текстові, графічні, звукові, відео;

в) залежно від умов доступу: безумовно відкриті; відкриті за умови аутентифікації користувача, наявності облікового запису, електронно-цифрового підпису тощо; платні;

г) за рівнем достовірності: достовірні; неперевірені; неправдиві (фейкові);

ґ) залежно від автора/власника (володільця) джерела: офіційні; приватні; керовані ботами; анонімні.

Усі вищевказані джерела можуть містити криміналістично значущу інформацію, яка і є предметом кіберрозвідки на основі відкритих джерел.

Вказану криміналістичну інформацію своєю чергою доцільно розподілити на категорії:

– про події та діяння, які містять ознаки кримінального правопорушення (вчиненого або такого, що готується) або які мають орієнтуюче чи доказове значення для кримінального провадження (наприклад, інформація про перебування підозрюваного за кордоном у момент вчинення кримінального правопорушення; факти, зафіксовані камерами відеоспостереження, і т.п.);

– про способи вчинення кримінальних правопорушень або способи підготовки до їх вчинення (інструкції щодо виготовлення вибухових пристроїв, наркотичних засобів тощо);

– інформація, що є закликом, підбурюванням чи схилянням до вчинення кримінального правопорушення (в тому числі оголошення щодо залучення до незаконної діяльності);

– інформація, обіг та поширення якої заборонено або обмежено (наприклад, продукція порнографічного характеру; продукція, яка пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України тощо);

– про осіб (які обґрунтовано підозрюються у вчиненні або причетності до вчинення кримінальних правопорушень, свідків, розшукуваних осіб та ін.), коло їхніх зв'язків, інтереси, спосіб життя, маршрути пересування, місця відвідування, поточне місцезнаходження, а також інформація, яка дає змогу ідентифікувати окремих осіб (наприклад, активістів під час масових заворушень, осіб, які дестабілізують оперативну обстановку у відповідному регіоні) тощо;

– про речі, які були предметом злочинного посягання або засобом/знаряддям вчинення кримінального правопорушення (місцезнаходження викраденого; зображення автомобіля, яким пересувалися особи, причетні до вчинення кримінального правопорушення; підроблені платіжні картки тощо), а також речі та предмети, обіг яких заборонено або обмежено (наркотичні засоби, зброя та ін.);

– про місцезнаходження об'єктів чи осіб у певний період часу (дані геолокації, картографічні дані);

– про фонові явища (сукупність аморальних проявів, які суперечать загальноприйнятим нормам поведінки та які органічно взаємопов'язані зі злочинністю, оскільки детермінують одне одного і тягнуть за собою соціальну деградацію особи (Ivanov & Dzhuzha, 2006: 257).

Зазначена інформація дає змогу суб'єктам кіберрозвідки:

а) орієнтуватися в суб'єктивній та об'єктивній стороні злочинного явища;

б) планувати оперативно-розшукові заходи, слідчі (розшукові) дії, власні дії та стратегію поведінки;

в) відстежувати результати вжитих оперативно-розшукових заходів, слідчих (розшукових) дій;

г) прогнозувати плин подій, дій;

ґ) вибирати найбільш ефективні методи впливу на суб'єктів злочину;

д) вживати превентивні заходи;

е) якісно виконувати професійні функції (Korystin et al., 2019: 155).

Процес кіберрозвідки на основі відкритих джерел включає в себе послідовність таких етапів, як визначення мети і завдань кіберрозвідки, планування, пошук, збирання та обробка інформації, отриманої з відкритих джерел, її аналіз та оцінка, формування висновків та підготовка результатів. Розглянемо більш детально кожен із цих етапів.

1. Визначення мети і завдань кіберрозвідки. На цьому етапі необхідно чітко визначити, які відомості про які саме об'єкти потрібно отримати в результаті проведення кіберрозвідки. На підставі інформаційних потреб чітко формулюється інформаційний запит, тобто складається

список запитань, на які необхідно знайти відповіді. Інакше в результаті розвідки можна отримати зовсім не ті дані, котрі необхідні для досягнення поставленої мети.

2. Планування. Це один із найбільш важливих етапів, на якому потрібно визначити інструменти та прийоми OSINT, що будуть застосовуватися для пошуку необхідної інформації. Також під час планування визначаються засоби безпеки (браузери, в тому числі VPN, які будуть використовуватися під час пошуку), а також заходи конспірації (створюють фейкові профілі в соціальних мережах, скриньки електронної пошти, вибирають сім-карти мобільних операторів, які будуть зазначені в акаунтах), котрі будуть вживатися під час пошуку інформації. Далі визначаються основні джерела (бази даних, соціальні мережі, сайти оголошень тощо), серед яких буде здійснюватися пошук необхідних даних. Із цією метою доцільно використовувати типові алгоритми пошуку інформації щодо певних осіб чи об'єктів або ж скласти власний алгоритм пошуку відповідно до раніше визначених мети і завдань кіберрозвідки. Досить ефективною також є візуалізація усіх запланованих дій та вихідних даних, зокрема, шляхом створення так званих «MindMaps» (дорожніх карт) із використанням спеціалізованих додатків, наприклад, XMind (Golushko & Driannykh, 2019: 159).

3. Пошук, збирання та обробка інформації. Пошук інформації – це процес взаємодії людини та масиву інформації, який полягає в сукупності логічних і технічних операцій, що реалізуються з метою відшукання документованої інформації, фактів і даних, релевантних запиту користувача (Eremenko et al., 2015: 110). Пошук може бути повнотекстним (здійснюється за допомогою пошукових систем Інтернету, наприклад www.google.com), за метаданими (за деякими атрибутами документа, що підтримується системою, як то назва документа, дата створення, розмір, автор тощо), за зображеннями (пошукова система розпізнає зміст зображення, завантаженого користувачем, відшукуючи схожі зображення) (Sukhyi, Milenin & Taradainik, 2015: 24).

Під час пошуку інформації необхідно користуватися сукупністю різноманітних прийомів і методів побудови пошукових запитів, різноманітними пошуковими системами. Крім того, варто звертати увагу на можливість пошуку інформації різними мовами, а також пошук видаленої інформації (шляхом перегляду кеш-версій сторінок або спеціалізованих сайтів, на яких зберігають архівні копії вебсторінок).

Пошук криміналістично значущої інформації може також здійснюватися шляхом моніторингу відкритих джерел інформації – структурованого огляду (системи спостережень) у відкритих джерелах інформації за станом визначеного об'єкта, який дозволяє швидко отримати уявлення про відображення конкретного об'єкта у відкритих джерелах інформації для подальших статистичних та аналітичних досліджень (Honchar, 2012: 69).

Збирання інформації полягає в повному вилученні її з джерела та надійному збереженні у зручному для подальшого опрацювання вигляді та відповідному форматі. Нині існує значна кількість інструментів, які дозволяють вилучити та копіювати усю розмішену на вебсторінці інформацію, а також зберігати її як у неструктурованому, так і у структурованому вигляді, зокрема в таблицях формату Excel (наприклад, копіювання усіх коментарів під дописами користувача соціальної мережі із зазначенням їх авторів, дати створення тощо).

Надалі зібрана інформація підлягає обробці, яка включає в себе перевірку даних із недостовірних джерел, порівняння інформації, отриманої з кількох джерел, виокремлення застарілих відомостей, видалення інформаційного шуму та виключення нерелевантних даних (Hassan & Hijazi, 2018: 343). Крім того, обробка передбачає встановлення додаткових прихованих даних (геоміток, відомостей про дату і час створення файлу, інформацію про прилад, яким було зроблено фотографію, ім'я користувача, який редагував зображення, і т.п.), а також відновлення пошкодженої інформації або зображень низької якості.

4. Аналіз та оцінка отриманих даних. Загалом аналіз інформації, отриманої з відкритих джерел, – це процес обробки певного масиву інформації з відкритих джерел, який полягає

в перетворенні знайденої розвідувальної інформації на кінцеві розвідувальні дані з метою приведення розрізнених відомостей про об'єкт розвідки в логічно обґрунтовану систему залежностей (просторово-часових, причинно-наслідкових тощо) (Honchar, 2012: 69).

Найбільш поширеними методами аналізу отриманої інформації є лексичний аналіз, семантичний аналіз, геоспросторовий аналіз та аналіз соціальних мереж (Yogish Pai & Krishna Prasad, 2021). У результаті проведеного аналізу насамперед необхідно відповісти на питання, чи була досягнута мета кіберрозвідки та виконані усі завдання, які ставилися перед початком її проведення. Оцінювати отриману інформацію слід за критеріями повноти, точності, оперативності, релевантності та вартості (Eremenko et al., 2015: 110).

5. Формування висновків та підготовка результатів. Після проведення аналізу та оцінки отриманих даних формулюються висновки за результатами та надаються рекомендації. Уся отримана інформація презентується у зручній для сприйняття формі.

Висновки. Узагальнюючи вищевикладене, зазначимо, що розвиток сучасних інформаційних технологій зумовлює необхідність застосування методу розвідки на основі відкритих джерел, розміщених у кіберпросторі, для отримання криміналістично значущої інформації, яка надалі може використовуватися для вирішення завдань, спрямованих на виявлення, розкриття та розслідування кримінальних правопорушень, встановлення місцезнаходження розшукуваних осіб. Процес кіберрозвідки на основі відкритих джерел включає в себе п'ять взаємопов'язаних етапів: визначення мети і завдань кіберрозвідки; планування; пошук, збирання та обробка інформації, отриманої з відкритих джерел; її аналіз та оцінка; формування висновків та підготовка результатів. Детально розглянувши вказані етапи в нашій статті, зауважимо, що подальшого наукового дослідження потребують прийоми та інструменти кіберрозвідки, які застосовуються на кожному із цих етапів.

References:

1. Adams, S. (2020). An introduction to OSINT and III. Retrieved from https://www.intelligencewithsteve.com/post/an-introduction-to-osint-and-iii.
2. Ataian, A.M., Gureva, T.N. & Sharabaeva, L.Iu. (2021).Tcifrovaia transformatciia vysshego obrazovaniia: problemy, vozmozhnosti, perspektivy i riski [The digital transformation of higher education: challenges, opportunities, prospects and risks]. *Otechestvennaia i zarubezhnaia pedagogika, Domestic and foreign pedagogy,* Vol. 1, 2(75), 7–22 [in Russian].
3. Bilous, V.V. (2015). Open Data i OSINT yak aktualni katehorii informatsiinoho zabezpechennia rozsliduvannia zlochyniv [Open Data and OSINT as current categories of criminal investigation information]. *Informatsiine zabezpechennia rozsliduvannia zlochyniv, Information support of crime investigation*: proceedings of the III International Round Table. 27-34, May, 29, 2015, Odesa: Yurydychna literatura [in Ukrainian].
4. Dodonov, A.G., Lande, D.V., Tcyganok, V.V., Andreichuk, O.V., Kadenko, S.V. & Graivoronskai a, A.N. (2017). Raspoznavanie informatcionnykh operatcii [Recognising information operations]. Kiev : OOO «Inzhiniring» [in Russian].
5. Eremenko, V.T., Minaev, V.A., Fisun, A.P., Konstantinov, I.S., Koskin, A.V., Belevskaia, Iu.A., Dvoriankin, S.V., Rytov, M.Iu. & Pavlinov I.A. (2015). Teoriia informatcii i informatcionnykh protcessov [Theory of information and information processes]. Orel: Gosuniversitet [in Russian].
6. Fedchak, I.A. (2021). Osnovy kryminalnoho analizu [Fundamentals of criminal analysis]. Lviv : Lvivskyi derzhavnyi universytet vnutrishnikh sprav [in Ukrainian].
7. Gibson, S.D. (2007). Open Source Intelligence (OSINT): a contemporary intelligence lifeline: *PhD Tesis*. Cranfield University. Retrieved from http://dspace.lib.cranfield.ac.uk/handle/1826/6524
8. Golushko, A.P. & Driannykh, Iu.Iu. (2019). Tcel i zadachi poiska informatcii v otkrytykh istochnikakh (open source intelligence) [Purpose and objectives of open source intelligence]. *Vnedrenie rezultatov innovatcionnykh razrabotok: problemy i perspektivy, Implementing the*

results of innovative developments: problems and prospects : collection of articles from the international scientific and practical conference. 158–161. [in Russian].
9. Hassan, N.A., & Hijazi, R. (2018). Open Source Intelligence Methods and Tools. DOI: https://doi.org/10.1007/978-1-4842-3213-2_1
10. Honchar, R.O. (2012). Monitorynh ta analiz vidkrytykh dzherel informatsii yak sposib oderzhannia rozviduvalnoi informatsii orhanamy rozvidky Vnutrishnikh viisk [Monitoring and analysis of open sources of information as a way to obtain intelligence information from the intelligence agencies of the Internal Troops]. *Chest i zakon, Honor and Law,* 4(43), 67-73 [in Ukrainian].
11. Ivanov, Yu.F. & Dzhuzha, O.M. (2006). Kryminolohiia [Criminology]. Kyiv: Palyvoda A.V. [in Ukrainian].
12. Korystin, O.Ie., Svyrydiuk, N.P., Tsilmak, O.M., Zaiets, O.M., Ismailov, K.Iu. & Nekrasov, V.A. (2019). Taktychnyi kryminalnyi analiz: teoriia ta praktyka [Tactical criminal analysis: theory and practice]. Odesa: RVV ODUVS [in Ukrainian].
13. Selianko. J. (2001). NATO Open Source Intelligence Handbook. Retrieved from https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook
14. Shishliakov, D.V. (2017). Razvedka na osnove otkrytykh istochnikov [Open source intelligence]. *Ob aktualnykh problemakh voenno-professionalnoi deiatelnosti na inostrannykh iazykakh*, *On current problems of military professional activities in foreign languages*: collection of materials of the scientific-practical conference. 109–112, Sankt-Peterburg [in Russian].
15. Sukhyi, O.L., Milenin, V.M. & Taradainik, V.M. (2015). Alhorytmy poshuku v informatsiinykh systemakh [Search algorithms in information systems]. Kyiv. [in Ukrainian].
16. Tlumachnyi slovnyk ukrainskykh terminiv. Slovnyky terminiv: ukrainsko-anhlo-rosiiskyi, russko-ukraynsko-anhlyiskyi, english-russian-ukrainian (2004). [Explanatory dictionary of Ukrainian terms. Dictionaries of terms: Ukrainian-English-Russian, Russian-Ukrainian-English, English-Russian-Ukrainian] NP 306.7.086-2004. Kyiv : Derzhavnyi komitet yadernoho rehuliuvannia Ukrainy [in Ukrainian].
17. Williams, H.J., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. DOI: https://doi.org/10.7249/RR1964
18. Yarovoi, T.S. (2019). OSINT, yak perspektyvnyi instrument kontroliu za lobistskoiu diialnistiu v konteksti derzhavnoi bezpeky [OSINT as a prospective tool of lobbying control in the context of state security]. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia, Expert: paradigms of legal sciences and public administration,* 4(6), 201-208, Kyiv : Vydavnytstvo Lira. DOI: https://doi.org/10.32689/2617-9660-2019-4(6)-201-208 [in Ukrainian].
19. Yogish Pai, U. & Krishna Prasad, K. (2021). Open Source Intelligence and its Applications in Next Generation Cyber Security – A Literature Review. International Journal of Applied Engineering and Management Letters (IJAEML), 5(2), 1–25. DOI: http://doi.org/10.5281/zenodo.
20. Zakon Ukrainy "Pro dostup do publichnoi informatsii": vid 13 sichn. 2011 r. No. 2939-VI [Law of Ukraine "About access to public information" from January 13, 2011, No. 2939-VI]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2939-17#Text [in Ukrainian].
21. Zakon Ukrainy "Pro informatsiiu": vid 02 zhovt. 1992 r. No. 2657-XII [Law of Ukraine "About information" from October 02, 1992, No. 2657-XII]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].