УДК 341.1
DOI https://doi.org/10.24144/2788-6018.2025.02.134

ІНСТРУМЕНТИ OSINT: ФІКСАЦІЯ ВОЄНИХ ЗЛОЧИНІВ В УКРАЇНІ

Тома М.Г.,
кандидат юридичних наук,
доцент кафедри кримінального права,
Чернівецький національний університет імені Юрія Федьковича
ORCID: 0000-0001-50817842

Василова О.В.,
кандидат юридичних наук,
асистент кафедри кримінального права,
Чернівецький національний університет імені Юрія Федьковича
ORCID: 0000-0002-3023-5172

Тома М.Г., Василова О.В. Інструменти OSINT: фіксація воєнних злочинів в Україні.
Стаття присвячена аналізу інструментів OSINT (розвідки з відкритих джерел) та їх застосування, як перспективного інструменту моніторингу фіксації воєнних злочинів в контексті забезпечення національної безпеки. Автор розглядає, як вітчизняний, так і закордонний досвід у підходах до збору інформації через відкриті джерела, а також пропонує перелік найвідоміших інструментів OSINT. З урахуванням зростання потреби в Україні у фіксації воєнних злочинів, запропоновано ряд найефективніших інструментів у фіксації правопорушень, спрямованих на забезпечення справедливого розслідування та захист національних інтересів і гарантування національної безпеки. У ході дослідження визначено переваги використання OSINT. Серед яких, суттєва економія часу та ресурсів завдяки збору первинної інформації з відкритих джерел про діяльність суб'єктів воєнних злочинів; можливість надання керівництву країни якісно опрацьованої аналітичної інформації про потенційно небезпечні дії з боку рф, а також публічне поширення даних про порушення законодавства з боку рф, що завдяки відкритому характеру інформації, дозволить не лише протидіяти інформаційним атакам, але й встановити правосуддя. Ефективність OSINT у діяльності правоохоронних органів додатково підсилюватиметься завдяки міждисциплінарному складу фахівців цієї установи. Співвідношення між правом і OSINT, правом та діяльністю у сфері національної безпеки, а також правом і роботою правоохоронних органів базується на пріоритетності права над цими сферами. Відповідно, принцип верховенства права беззаперечно слугує ключовим принципом функціонування OSINTу контексті національної безпеки. Особливу увагу зосереджено на таких засадах: безперервність, поєднання відкритих і прихованих методів та засобів, підконтрольність і підзвітність діяльності розвідувальних органів, а також на дотриманні безсторонності й справедливості. На думку автора, активна інтеграція OSINT у роботу правоохоронної системи може стати важливим чинником ефективного регулювання правоохоронної діяльності в Україні, особливо в аспекті забезпечення національної безпеки.
Ключові слова: відкриті джерела, розвідка, інформація з відкритих джерел, OSINT, збір розвідданих, національна безпека, розслідування.

Toma M.G., Vasylova O.V. OSINT tools: recording war crimes in Ukraine.
The article is devoted to the analysis of OSINT (open source intelligence) tools and their application as a promising tool for monitoring the recording of war crimes in the context of ensuring national security. The author considers both domestic and foreign experience in approaches to collecting information through open sources, and also offers a list of the most famous OSINT tools. Attention is paid to the classification of sources that are suitable for use within the framework of this methodology. Taking into account the growing need in Ukraine for recording war crimes, a number of the most effective tools for recording offenses aimed at ensuring a fair investigation and protecting national interests and guaranteeing national security are proposed. The study identified the advantages of using OSINT. Among them: significant savings in time and resources due to the collection of primary information from open sources about the activities of war crime subjects; the ability to provide the country's leadership with high-quality analytical information about potentially dangerous actions by the Russian Federation; as well as public dissemination of data on violations of the law by the Russian Federation, which, due to the open nature of the information, will allow not only to counteract information attacks, but also to establish justice. The effectiveness of OSINT in the activities of law enforcement agencies

will be further enhanced due to the interdisciplinary composition of specialists of this institution. The relationship between law and OSINT, law and activities in the field of national security, as well as law and the work of law enforcement agencies is based on the priority of law over these areas. Accordingly, the principle of the rule of law undoubtedly serves as a key principle of the functioning of OSINT in the context of national security. Particular attention is focused on the following principles: continuity, a combination of open and covert methods and means, control and accountability of the activities of intelligence agencies, as well as adherence to impartiality and fairness. In the author's opinion, the active integration of OSINT into the work of the law enforcement system can become an important factor in the effective regulation of law enforcement activities in Ukraine, especially in terms of ensuring national security.

Key words: open sources intelligence, open source information, OSINT, intelligence gathering, national security, investigation.

Постановка проблеми. Сьогодні інструменти OSINT перетворилися на важливий елемент роботи засобів масової інформації, особливо у контексті висвітлення російсько-української війни. Інструменти OSINT пропонують широкий спектр можливостей, починаючи від збору та аналізу даних до забезпечення надійності інформації, протидії ворожій дезінформації та пропаганді, а також укріплення довіри до медіа, що є надзвичайно важливим. Крім того, сучасним працівникам правоохоронних органів, тепер легше розслідувати воєнні злочини та будувати свої докази, фіксовані інструментами OSINT, та притягнути воєнних злочинців до кримінальної відповідальності за злочини проти людства. OSINT є ефективним інструментом, який допомагає працівникам правоохоронних органів оперативно реагувати на актуальні події. Наприклад, під час оборони Києва в перші дні повномасштабного вторгнення активно використовувалися дописи з соціальних мереж і супутникові знімки для підтвердження або спростування інформації про бойові дії, руйнування інфраструктури та переміщення військової техніки. Завдяки цьому вдалося запобігти поширенню паніки серед мирного населення та забезпечити передачу виключно перевірених фактів.

Мета дослідження: з'ясувати, які інструменти OSINT використовують працівники правоохоронних органів у фіксації злочинів під час повномасштабної війни з рф.

Стан опрацювання проблеми. Інструменти OSINT стали предметом дослідження багатьох вітчизняних науковців: О.Ф. Андрійко, О.М. Бандурка, Т.О. Коломоєць, В.К. Колпаков, В.І. Литвиненко, С.Я. Тихон, Т.П. Пащенко, О.В. Минько та ін.

Виклад основного матеріалу. На сьогоднішній день під час невиправданої та нічим неспровокованої російської агресії виникає новий вимушений фронт у боротьбі на шляху до справедливості. І цей фронт знаходиться не в межах суходолу ліній фронту, а в цифровому його вимірі. Скрупульозна перевірка картин/зображень та відео- наслідків ракетних ударів чи кривавих доказів надлюдських знущань/страт - стає цілком гідним інструментом в арсеналі розслідування та судового переслідування воєнних злочинців. Матеріали, які відображаються у фотознімках та відео, є невід'ємними доказами невимовних жахіть, несуть у собі потенціал для майбутнього визначення джерел агресії та деталей скоєних воєнних злочинів.

На тлі кривавого сьогодення в технологічних прогресіях у сфері масової інформації, щоденно, в побуті набуває своєї популярність визначення поняття OSINT. Вказана абревіатура розтлумачується як Open Source INTelligence, що в перекладі розуміється як відкриті джерела інформації/відомостей або ж як відкриті джерела розвідки. Наукові джерелах зазначають, що OSINT це:

– діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору [1];

– діяльність по отриманню розвідувальної інформації з відкритих джерел [2];

– розвідка на основі аналізу відкритих джерел інформації [3];

– діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору, розвідка на основі аналізу відкритих джерел інформації [4].

Збирання інформації, її перевірка та, у свою чергу, оцінка цифрових даних, що містить докази воєнних злочинів, вчинених під час збройної агресії на території нашої держави, являють собою складний лабіринт, з якого ми маємо знайти вихід. Такі виклики включають у собі технічні, етичні та правові аспекти, вимагаючи різноманітних стратегій для ефективного їх рішення. Чисельна кількість цифрового контенту, який існує на сьогоднішній день, що створюється під час війни в Україні, включаючи відеоспостереження, знімки та різного роду пости в соціальних мережах, формує нові виклики для фіксації та збору існуючої інформації. Гарантування автентичності та збереження цих даних серед цілковитого хаосу неоголошеної війни є надскладним, архіважливим завданням сьогодення. Розпізнати справжні докази від шахрайського/ або фальшивого контенту стає все складніше.

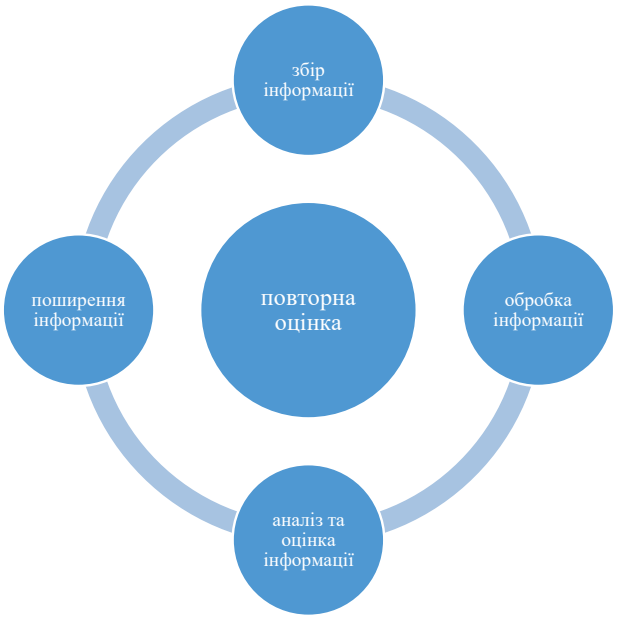
В умовах, у яких знаходиться наша країна на сьогоднішній день одержання достовірної інформації в найкоротші терміни є важливим та необхідним не тільки для Збройних сил України, але й

для підрозділів Національної поліції, Служби безпеки України та інших підрозділів, які здійснюють підслідність. Саме тому все частіше зустрічаємо інформацію, що правоохоронні органи використовують різні технологічні методи збору інформації, а також методи **OSINT** в своїй службовій діяльності.

Стаття 1 Закону України «Про інформацію» говорить нам, що інформація являє собою будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Отже, таким чином законодавець відносить до суті інформації «відомості та/або дані», що представляють собою саме інформацію, перероблену в певну форму представлення, тобто, вищезазначені дані або відомості, а не інформація як знання про різні факти, події та речі, які, у свою чергу, не є інформацією в чистому вигляд [5].

Діяльність **OSINT** також дає можливість отримувати доступ до електронних даних, таких зокрема як, листування, документи або ж інші електронні записи, які в свою чергу можуть становити доказову базу в кримінальному провадженні, щодо воєнних злочинів. Крім того, за допомогою методів **OSINT можна** фіксувати та ідентифікувати самих суб'єктів вчинення злочинів, та в результати мати змогу притягнути їх до відповідальності.

OSINT відноситься до процесу збору інформації з загальнодоступних джерел, насамперед таких як соціальні медіа, різноманітні агентства новин, урядові записи та супутникові знімки. Структура реалізації методу **OSINT** можливо представити у вигляді різних етапів або різних фаз, які утворюють ланцюговий ефект, утворюючи циклічне коло:



Прогнозується, що ринок OSINT демонструватиме суттєве зростання упродовж наступних п'яти років, відкриваючи широкі перспективи для стартапів, які прагнуть зайняти свою нішу в цій сфері.

Ось декілька ключових інструментів, що використовуються для розвідки з відкритих джерел:

Maltego-це багатофункціональна платформа розвідки з відкритим кодом, створена для оптимізації та прискорення розслідувань. Вона забезпечує доступ до 58 джерел даних, функцію ручного завантаження та базу, яка підтримує до 1 мільйона об'єктів, що дозволяє проводити більш глибокий аналіз. Потужні засоби візуалізації Maltego пропонують різноманітні макети, як-от блокові, ієрархічні або кругові графіки, доповнені вагами й примітками для кращого опрацювання інформації.

Використовуючи Maltego, команди з довіри та безпеки, співробітники правоохоронних органів і фахівці з кібербезпеки отримують можливість швидко генерувати результати розслідувань з доступною та зручною для аналізу інформацією.

Spiderfoot-це відкритий інструмент для OSINT-розвідки, який пропонує широкий набір можливостей. Він дозволяє здійснювати збір і аналіз даних, таких як, IP-адреси, діапазони CIDR, домени та субдомени, ASN, електронні адреси, телефонні номери, імена, імена користувачів, адреси BTC та багато іншого.

OSINT Framework-це відмінний інструмент для збору розвідувальної інформації на основі відкритих джерел. Він охоплює практично все, починаючи від великої бази даних із джерелами до корисних посилань на функціональні інструменти, що значно полегшує процес дослідження порівняно з окремим аналізом кожної програми чи утиліти окремо.

Каталог також пропонує ресурси для операційних систем, не обмежуючись лише Linux, забезпечуючи рішення для широкого спектра потреб. Основна складність полягає у створенні ефективної стратегії пошуку, яка дозволяє звузити результати до конкретних завдань, таких як визначення реєстрації транспортного засобу або пошук електронної адреси. Проте, завдяки чіткій організації він стає незамінним інструментом, який значно розширює можливості користувача.

Lampyre - це комерційне програмне забезпечення, орієнтоване на OSINT, що надає потужні інструменти для перевірки контрагентів, аналізу кіберзагроз, розслідування злочинів та фінансової аналітики. Програма вирізняється інтуїтивно зрозумілим інтерфейсом і можливістю швидкого встановлення на комп'ютер одним кліком або запуску онлайн без зайвих труднощів.

Вона дозволяє розпочати аналіз із базової точки даних, такої як реєстраційний номер компанії, ім'я або номер телефону, і автоматично обробляє інформацію з понад 100 постійно оновлюваних джерел для отримання цінної аналітики.

Користувачі можуть взаємодіяти з даними через настільний додаток або за допомогою API-запитів. Крім цього, для компаній, які потребують масштабованого рішення для управління ризиками та дослідження загроз, SaaS-пропозиція Lampyre під назвою Lighthouse дозволяє оплачувати використання послуг через виклики API.

Recon-ng є потужним інструментом збору інформації, спрямованого на дослідження, пов'язані з веб-доменами. Із початкового стану простого сценарію він еволюціонував у повноцінний фреймворк із широкими можливостями. Завдяки його функціоналу користувачі мають змогу здійснювати ідентифікацію вразливостей веб-ресурсів, проводити аналіз GeoIP, вивчати DNS-записи та здійснювати сканування відкритих портів.

Інструмент особливо корисний для виявлення конфіденційних файлів, таких як, robots.txt, пошуку прихованих субдоменів, ідентифікації помилок SQL, а також для збору інформації про систему управління контентом (CMS) компанії чи даних WHOIS.

Aircrack-ng – це потужний і багатофункціональний інструмент, який широко використовується фахівцями з цифрової безпеки для перевірки захищеності бездротових мереж. Він дозволяє здійснювати моніторинг мереж, збирати пакети, аналізувати кадри, а також отримувати WEP IV та інформацію про розташування точок доступу за підтримки GPS.

Інструмент також виконує тести на проникнення в мережі та оцінює їхню стійкість за допомогою атак із введенням маркерів, створенням фальшивих точок доступу чи використанням та повторення даних. Крім того, він здатний підбирати паролі як для протоколу WEP, так і для WPA PSK (версіїWPA 1 і 2). Завдяки цьому Aircrack-ng стає незамінним рішенням для виявлення потенційних вразливостей в мережах до виникнення загроз. Головною перевагою даного інструмента є його універсальність.

Хоча спочатку він був розроблений під Linux, його адаптовано і для інших операційних систем, таких як Windows, macOS та FreeBSD. Додатково інтерфейс командного рядка (CLI) відкриває можливість тонкого налаштування функціоналу. Це ідеально підходить для досвідчених користувачів, які можуть створювати власні сценарії, щоб кастомізувати інструмент та розширювати його можливості.

Metagoofil- це безкоштовний інструмент, доступний на GitHub, який спеціалізується на вилученні метаданих із різноманітних публічних документів, такихяк .pdf, .doc, .ppt і .xls. Завдяки своїй високій ефективності, він може витягувати такі корисні дані, як імена користувачів, справжні імена, а також інформацію про сервери та шляхи до файлів, пов'язаних із цими документами.

Крім того **OSINT** дає можливість проводити online-розслідування та віднайти цифрові сліди кримінальних правопорушень, доповнюючи дані з супутника.

Різні за розміром обсяги інформації, необхідні для порушення кримінального провадження, так і для подальшого розслідування воєнних злочинів та злочинів проти людяності, вже знаходяться у відкритому доступі. Просто відповідна інформація та її частини/фрагменти знаходиться ніби у тіні. Спеціалісти, що працюють у **OSINT** фрагментарно збирають цю інформацію у загальну картину відтворюючи реальність. До прикладу, з відкритих джерел ми дізнаємося про рух військових рф, зброї, стратегію ворога і навіть можемо дізнатись їхні майбутні кроки.

Попри безцінні переваги **OSINT** у фіксації та розслідуваннях воєнних злочинів, його інтеграція методів в судові процедури є надскладною. Найважливіші виклики включають: встановлення фактичних реальних даних цифрових доказів, тому що суд повинен бути переконаним, що докази є реальними і не були підроблені або зманіпульовані; джерела з якого було отримано інформацію мають бути надійними та перевіреними, з метою недопущення їх оскарження; підтримання циклічності ланцюжка збереження цифрових доказів, в цілях недопущення порушення питання щодо їх цілісності; проблеми секретності, зокрема, у разі ідентифікації осіб, які можуть не бути безпосередньо залучені до конфлікту тощо. Для вирішення цих проблем та вдосконалити допустимість

доказів **OSINT** у суді, варто вжити кілька заходів, зокрема, збирання та перевірки доказів та звичайно налагодження співпраці між практиками **OSINT** та слідчо-оперативними групами.

Враховуючи неоціненний внесок роботи **OSINT**, він відіграє критичну функцію у виявленні та документуванні різноманітних доказів воєнних злочинів під час збройної агресії рф в Україні, його можливості у використані загальнодоступної інформації змінила методи підходу у розслідувані порушень прав людини та воєнних злочинів.

Висновки. Прогрес у застосуванні технологій OSINT, супутникових знімків та кіберзброї для документування воєнних злочинів значною мірою визначається ефективністю збору даних, їх належним зберіганням та забезпеченням захисту. Контроль доступу до даних, відповідне збереження на захищених серверах та ефективний аналіз запорука ефективних розслідувань. Програмне забезпечення для Open Source Intelligence (OSINT) набуває все більшого значення як інструмент для збору загальнодоступної інформації з різних відкритих джерел, серед яких пошукові системи, соціальні мережі йофіційні державні документи. Завдяки використанню передових алгоритмів, OSINT-інструменти здатні здійснювати перехресний аналіз даних, що дозволяє отримувати точну інформацію та виявляти раніше недоступні взаємозв'язки.

Застосування методів OSINT у розкриті воєнних злочинів має вагомий потенціал, однак вимагає узгоджених дій та юридичної уваги у подальшому. Завдяки цифровим технологіям ми можемо розраховувати на об'єктивне правосуддя та вимагати справедливий суд над російськими окупантами за воєнні злочини, сприяти міжнародному розголосу та наближати нашу перемогу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. Протидія кіберзлочинності та торгівлі людьми: Збірник матеріалів Міжнародної науково-практичної конференції (м. Харків, 27 травня 2020 року). С. 135–137.
2. Яровой Т.С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*, 2019, № 4(6). С. 201–208.
3. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021, № 9. С. 332–334.
4. Минько О.В., Іохов О.Ю., Оленченко В.Т., Власов К.В. Використання технологій OSINT для отримання розвідувальної інформації. *Експерт: парадигми юридичних наук і державного управління*, 2019, № 4(6). С. 201–208.
5. Бакумов О.С., Марчук М.І., Гудзь Т.І., Венглінський О.О. Інформація: до питання про змістову еволюцію терміна. *Право і безпека – Право и безопасность – LawandSafety.* 2021. No 3 (82). С. 24. URL: https://pb.univd.edu.ua/index.php/PB/ article/view/494/385.