14. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21.10.2015 № 835.

15. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.

## OSINT У ПРОЦЕСАХ КІБЕРРОЗВІДКИ (CYBER THREAT INTELLIGENCE, CTI)

***Никитенко Альбіна***
*здобувачка вищої освіти Інститут права та безпеки*
*Одеський державний університет внутрішніх справ*
*Науковий керівник**: Грезіна Олена Миколаївна***
*доктор філософії в галузі права,*
*доцент кафедри кримінального аналізу*
*та інформаційних технологій*
*Одеський державний університет внутрішніх справ*

OSINT— розвідка на основі відкритих джерел — це методологія збору, обробки та аналізу загальнодоступної інформації з метою отримання розвідувальних даних [1]. OSINT охоплює пошук інформації, її реєстрацію, облік та аналіз, аналітико-синтетичну переробку первинної інформації та забезпечення безпеки інформаційних результатів.

У контексті Cyber Threat Intelligence (CTI) — кіберрозвідки загроз — OSINT є одним із ключових інструментів, що дозволяє організаціям виявляти, аналізувати та нейтралізувати потенційні кіберзагрози превентивно. CTI охоплює процеси збору даних про актуальні та потенційні кіберзагрози, тактики, техніки й процедури (TTP) зловмисників, а також відстеження відомих загрозливих акторів. OSINT забезпечує основу для цих процесів, оскільки значна частина розвідувальної інформації є публічно доступною [2].

У межах CTI фахівці використовують широкий спектр відкритих джерел. Технічні ресурси включають бази даних вразливостей (CVE, NVD), платформи індикаторів компрометації (IOC), репозиторії зловмисного програмного забезпечення (VirusTotal, MalwareBazaar), а також пошукові системи для виявлення

вразливих пристроїв (Shodan, Censys). Соціальні й комунікаційні джерела охоплюють форуми даркнету, Telegram-канали та спеціалізовані спільноти, де учасники обговорюють нові атаки, інструменти та вразливості [3].

В українському контексті важливу роль відіграє CERT-UA — Урядова команда реагування на комп'ютерні надзвичайні події України, яка публікує відкриті бюлетені про кіберактивність APT-груп (зокрема UAC-0001/APT28, UAC-0200), індикатори компрометації та рекомендації щодо захисту. Ці звіти є цінним публічним джерелом OSINT для аналітиків CTI [5]. Пасивна розвідка DNS, WHOIS-запити, аналіз сертифікатів SSL/TLS та метаданих документів дозволяють встановлювати інфраструктуру зловмисників [2].

Цикл кіберрозвідки складається з планування, збору, обробки, аналізу, поширення та зворотного зв'язку. OSINT інтегрується на кожному етапі: під час збору формуються автоматизовані фіди загроз; на етапі аналізу проводиться кореляція індикаторів компрометації з відомими кампаніями та атрибуція атак конкретним групам. Як зазначає сертифікований інструктор ISSP Training Center Юрій Самохвалов, навіть інформацію з відкритих джерел зловмисники активно використовують для планування атак, що зобов'язує захисників так само системно моніторити ці ж джерела [5].

Практичним прикладом у вітчизняному контексті є моніторинг фішингових кампаній через відстеження нещодавно зареєстрованих доменів. Аналітики CTI відстежують домени, що імітують легітимні організації, ще до початку атаки. Аналогічно, відстеження активності у підпільних форумах і Telegram-каналах дозволяє завчасно виявляти оголошення про продаж вкрадених облікових даних або доступу до корпоративних мереж. Такі платформи, як MISP та OpenCTI, дозволяють агрегувати та візуалізувати дані з множини OSINT-джерел [3].

Незважаючи на широкі можливості, OSINT у CTI має суттєві обмеження. У науковій статті Легомінової С. та ін. зазначається, що організації не можуть повністю запобігти збору даних про себе з відкритих джерел, однак зобов'язані бути готовими до протидії наслідкам такого збору [3]. Ключовою проблемою є значний обсяг інформаційного шуму — більшість зібраних даних потребує ретельної фільтрації та верифікації. Існують також правові та етичні ризики, пов'язані зі збором даних у «сірих зонах» мережі.

Атрибуція атак на основі лише відкритих джерел може бути хибною через використання техніки false-flag, коли зловмисники навмисно залишають сліди, що вказують на інших акторів [2].

OSINT є невід'ємною складовою сучасної кіберрозвідки, забезпечуючи аналітиків CTI критичними даними про загрози, актори та інфраструктуру зловмисників. Відкриті звіти CERT-UA, публікації дослідницьких платформ, дані з форумів та технічних реєстрів у сукупності формують потужну розвідувальну базу. Ефективне застосування методів OSINT дозволяє організаціям перейти від реактивного до проактивного підходу в кібербезпеці – виявляти загрози раніше, ніж вони завдадуть реальної шкоди [4;5].

**Список використаних джерел:**

1. Дрижакова Д., Волинець Р. Використання відкритих джерел інформації(OSINT) у сфері безпеки держави: технології та перспективи. Матеріали конференцій МЦНД. Дніпро, 2025. С. 138–141. URL: https://archives.mcnd.org.ua/index.php/conference-proceeding / article/view/599

2. Легомінова С., Щавінський Ю., Рабчун Д., Запорожченко М.,Будзинський О. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації.*Кібербезпека: освіта, наука, техніка*.2024. № 1(25). С. 294–303. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/630

3. Кіберрозвідка (I-OSINT CR): програма навчання. ISSP Training Center. URL: https://www.issp.training/programs/i-osint-cr

4. CERT-UA — Урядова команда реагування на комп'ютерні надзвичайніподії України. Звіти про кіберінциденти та бюлетені безпеки. URL: https://cert.gov.ua

5. Самохвалов Ю. Як працює OSINT-розвідка? Від бізнес-аналізу дооборони України.ISSP Training Center.2022. URL: https://www.issp.trai ning/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny