ВИКОРИСТАННЯ OSINT У ЦИФРОВИХ РОЗСЛІДУВАННЯХ КІБЕРІНЦИДЕНТІВ

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

Балацька Валерія
Доктор філософії
Львівський державний університет безпеки життєдіяльності

У сучасну епоху цифрових технологій обсяг інформації, що створюється та поширюється в Інтернеті, зростає експоненційно. Загальнодоступні дані з соціальних мереж, вебсайтів, онлайн-баз даних, публічних реєстрів та інших відкритих джерел містять величезну кількість інформації, яка може бути використана для розслідування кіберінцидентів і виявлення загроз. Саме цю інформацію досліджує дисципліна, відома як Open Source Intelligence (OSINT), що передбачає збір, обробку та аналіз відкритих джерел для отримання інтелектуальних висновків [1].

Методи OSINT сьогодні активно застосовуються в різних сферах: від національної безпеки й правоохоронної діяльності до корпоративної кібербезпеки та кримінальних розслідувань [5]. У контексті кіберінцидентів OSINT дозволяє експертам не лише виявляти та відстежувати атаки, але й отримувати цифрові докази, аналізувати поведінкові патерни зловмисників, розкривати мережеві зв’язки та виявляти вразливості в інфраструктурі [2].

З огляду на постійне зростання кількості кіберзлочинів і складності сучасних атак, використання OSINT стає не лише корисним, а й необхідним інструментом розслідування. Публічно доступні джерела дозволяють зменшити час реагування, доповнити дані традиційних цифрово-форензичних методів та створити більш повну картину подій під час інцидентів [3].

Використання OSINT у цифрових розслідуваннях є особливо актуальним у зв’язку зі зростанням кількості кібератак, що супроводжуються прихованим проникненням, використанням анонімізації та швидкою зміною інфраструктури зловмисників. У спрямованих кібератаках початкові етапи – проникнення, розвідка та закріплення – можуть тривати 6–12 місяців і залишатися непомітними, причому жертви часто бачать лише фінальну фазу атаки [4]. Традиційні методи цифрової криміналістики часто базуються на аналізі локальних носіїв інформації, журналів подій та мережевого трафіку, однак у багатьох випадках цього недостатньо для встановлення повного ланцюга атаки та ідентифікації причетних осіб. OSINT, у свою чергу, дозволяє доповнити форензичний аналіз даними із зовнішніх джерел, що суттєво підвищує ефективність розслідування.

Під час розслідування кіберінцидентів відкриті джерела можуть містити важливі цифрові сліди: доменні імена, IP-адреси, цифрові сертифікати, сліди реєстрації інфраструктури, згадки про фішингові кампанії, витоки облікових даних, а також інформацію про активність користувачів у соціальних мережах. Зокрема, аналіз DNS-даних, WHOIS-інформації, історії зміни доменів, пасивного DNS та сертифікатів TLS дозволяє виявити взаємозв'язки між ресурсами, які використовуються зловмисниками.

Крім того, OSINT-методи активно застосовуються для ідентифікації шкідливого програмного забезпечення та пов'язаної інфраструктури. Аналіз відкритих баз індикаторів компрометації (IOC), звітів компаній з кібербезпеки, форумів, даркнет-майданчиків та репозиторіїв шкідливих зразків дає змогу оперативно встановити тип атаки, можливу групу зловмисників та їхні типові тактики. Важливим елементом є також використання концепції MITRE ATT&CK, яка допомагає систематизувати зібрані дані та співвіднести їх з відомими техніками атак (рис.1).

Рисунок 1 – взаємозв'язок OSINT і концепції MITRE ATT&CK
Власна розробка авторів

Даний рисунок ілюструє взаємозв'язок між OSINT та концепцією MITRE ATT&CK у процесі цифрового розслідування кіберінцидентів. У лівій частині схеми показано, що OSINT базується на зборі інформації з відкритих джерел, таких як WHOIS і DNS-дані, звіти про шкідливе програмне забезпечення, списки індикаторів компрометації та ресурси даркнету. Ці дані самі по собі є фрагментарними, тому в схемі вони спрямовуються до центрального елемента OSINT, де відбувається їх узагальнення та первинний аналіз. Далі інформація перетворюється на threat intelligence, тобто аналітичні висновки, які можуть бути використані для практичного розслідування та оцінки загроз. У правій частині зображено матрицю MITRE ATT&CK, яка виступає як універсальна модель класифікації дій зловмисника. Зібрані через OSINT артефакти співвідносяться з відповідними тактиками і техніками, наприклад фішинговий домен може бути віднесений до етапу первинного доступу, шкідливі скрипти — до виконання або закріплення в системі, а викрадені облікові дані — до технік доступу до

облікових даних. Таким чином схема демонструє, що OSINT забезпечує джерельну інформацію для розслідування, а MITRE ATT&CK дозволяє структуровано інтерпретувати ці дані та відновити логіку атаки у вигляді послідовності дій зловмисника.

Окремої уваги заслуговує роль OSINT у процесі атрибуції кіберінцидентів. Хоча повна атрибуція часто потребує доступу до закритих даних або оперативної інформації, відкриті джерела дозволяють сформувати первинні гіпотези щодо походження атаки, її цілей, а також рівня підготовки зловмисників. Наприклад, аналіз часових зон активності, мовних особливостей у шкідливому коді чи фішингових повідомленнях, а також повторюваних шаблонів реєстрації доменів може допомогти у встановленні ймовірної належності до певної групи.

Рисунок 2 – роль OSINT у процесі атрибуції кіберінцидентів
Власна розробка авторів

Однак, застосування OSINT у цифрових розслідуваннях має низку обмежень (таблиця 1). Основними проблемами є достовірність та актуальність даних, можливість навмисної дезінформації, а також юридичні й етичні аспекти збору інформації. Надмірна довіра до відкритих джерел без підтвердження може призвести до хибних висновків або помилкової атрибуції. Тому OSINT доцільно розглядати як допоміжний інструмент, що повинен застосовуватись у комплексі з класичними методами цифрової криміналістики.

Таблиця 1. Обмеження застосування OSINT

№	Обмеження	Пояснення
1	Достовірність джерел	Не вся інформація з відкритих джерел є правдивою; може бути помилкова або свідомо маніпулятивна.
2	Актуальність даних	Дані можуть бути застарілими, що знижує їхню цінність для аналізу або прийняття рішень.
3	Юридичні обмеження	Збір і використання інформації може регулюватися законами про конфіденційність, авторські права та персональні дані.

4	Етичні межі	Використання OSINT не повинно порушувати моральні та етичні норми, наприклад, вторгнення в приватне життя.
5	Технічні обмеження	Доступ до деяких ресурсів може бути обмежений через платні підписки, CAPTCHA, блокування IP або шифрування.
6	Масивність даних	Велика кількість інформації ускладнює її обробку та аналіз без спеціальних інструментів.
7	Ризик дезінформації	Зловмисники можуть навмисно поширювати фейкові дані для введення в оману аналітиків.
8	Локалізаційні та мовні бар'єри	Інформація може бути недоступною через мовні обмеження або специфічні регіональні ресурси.
9	Вразливість до зміни джерел	Сайти та платформи можуть змінювати контент або видаляти його, що ускладню

Таким чином, OSINT є важливим компонентом сучасних розслідувань кіберінцидентів, оскільки дозволяє швидко отримати додаткову інформацію про загрози, інфраструктуру атак та можливих зловмисників. Комплексне поєднання OSINT та цифрової форензики забезпечує підвищення точності аналізу, скорочення часу реагування та формування більш повної доказової бази.

Список літератури:

1. Open-source intelligence. URL: https://en.wikipedia.org/wiki/Open-source_intelligence
2. Puchkov, O., Lande, D., Subach, I., Boliukh, M., & Nahornyi, D. (2021). OSINT investigation to detect and prevent cyber attacks and cyber security incidents. Information Technology and Security, 9(2), 209–218. https://doi.org/10.20535/2411-1031.2021.9.2.249921
3. Understanding OSINT: A Comprehensive Guide. URL: https://www.mcafeeinstitute.com/blog/understanding-osint-a-comprehensive-guide
4. Два роки після NotPetya. Кібератаки не припиняються ні на мить. URL: https://biz.nv.ua/ukr/experts/kiberataka-shcho-ce-take-i-yaki-jiji-naslidki-50036682.html
5. Полотай О.І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. Вісник ЛДУБЖД : зб. наук. праць. Львів : ЛДУБЖД, 2023. № 28. С. 73–80. https://doi.org/10.32447/20784643.28.2023.07