Лях І.М., магістрант
Державний університет «Житомирська політехніка»

СФЕРИ ЗАСТОСУВАННЯ OSINT У СУЧАСНИХ КІБЕРЗАГРОЗАХ

В епоху стрімкого розвитку цифрових технологій та зростання кіберзагроз важливу роль починає відігравати розвідка у відкритих джерелах (OSINT). Цей підхід дозволяє використовувати доступні інформаційні ресурси для моніторингу та аналізу загроз кібербезпеці як окремих осіб, так і великих корпорацій, державних установ або організацій.

Сучасний кіберпростір характеризується швидким зростанням обсягу даних і складністю кіберзагроз. У цьому контексті технології OSINT (розвідка у відкритих джерелах) стають важливим інструментом для виявлення, аналізу та протидії кіберзагрозам. OSINT дозволяє збирати та аналізувати дані з публічно доступних джерел, включаючи соціальні мережі, новинні ресурси, форуми, сайти організацій, що робить його ефективним засобом для моніторингу кіберризиків.

Основні сфери застосування OSINT в контексті завдань кібербезпеки включають :

1. **Моніторинг витоків даних**. OSINT дозволяє виявляти витоки конфіденційної інформації у відкритих джерелах, таких як форуми даркнету, соціальні мережі та онлайн-платформи обміну файлами. Наприклад, аналіз витоків даних, дозволяє здійснювати ідентифікацію осіб-зловмисників та військових злочинців.

Окремо слід зауважити, що OSINT-технології використовуються для так званого «doxing», коли без згоди особи, здійснюється збір персональної або конфіденційної інформації, з метою її подальшого несанкціонованого використання [1].

2. **Аналіз соціальної інженерії**. Використання OSINT допомагає досліджувати активність зловмисників у соціальних мережах та інших платформах для прогнозування можливих атак. Зокрема, аналіз активності допомагає передбачати потенційні атаки через методи соціальної інженерії, зокрема фішинг або шахрайські дії.
3. **Виявлення фішингових ресурсів**. Завдяки інструментам OSINT можливе автоматизоване виявлення шкідливих сайтів, які імітують легітимні ресурси, що забезпечує можливість блокування зловмисних ресурсів, ще до початку їх експлуатації та завдання шкоди користувачам.

Наразі спостерігається зростання кількості випадків, з використання тактики багатоетапного фішингу, яка заснована на перенаправленні користувача від одного ресурсу до іншого, аби уникнути виявлення.

За таких умов, використання OSINT-технологій дозволяє прогнозувати атаки на ресурси, а також хдійснювати дослідження випадкві

4. **Кіберрозвідка щодо атакуючих груп**. Застосування OSINT дозволяє ідентифікувати активності та атрибуцію груп зловмисників шляхом збору відкритих даних про їх діяльність. Це дає змогу зрозуміти їхню тактику, методи та цілі, а також атрибутувати конкретні атаки до певних груп.
5. **Оцінка інформаційної безпеки компаній**. За допомогою OSINT можна визначати слабкі місця корпоративних ресурсів, які доступні через Інтернет. Це можуть бути неправильні налаштування серверів, незахищені API або витік технічної інформації.
6. **Протидія дезінформації та інформаційним операціям.** OSINT сприяє ідентифікації інформаційних кампаній, спрямованих на дискредитацію компаній або державних органів. Моніторинг інформаційних потоків дозволяє виявити та нейтралізувати фейки.

Враховуючи вищезазначене, можна виокремити наступні шляхи розвитку застосування OSINT-технологій в кібербезпеці, зокрема:

- Автоматизація процесів пошуку інформації у відкритих джерелах та використання штучного інтелекту;
- Розширене використання OSINT у військовій сфері;
- OSINT у боротьбі з фінансовими злочинами;
- Юридичні та етичні аспекти OSINT.

Таким чином, OSINT є важливим компонентом комплексної системи кіберзахисту, що дозволяє завчасно ідентифікувати та запобігати кіберзагрозам.

Список використаних джерел:

1. Івкова, В. і Опірський, І. 2024. Дослідження проблематики забезпечення безпеки персональних даних та конфіденційної інформації в контексті протидії OSINT. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2, 26 (Груд 2024), 189–199. DOI:https://doi.org/10.28925/2663-4023.2024.26.682.
2. Брукс К. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. — 2020.
3. Коваленко О. А. Методи OSINT у задачах моніторингу кіберзагроз. Вісник кібербезпеки, 2022.