Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми «ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ДОБУВАННЯ КОРИСНОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ОНЛАЙН-ДЖЕРЕЛ ТА ЗАСОБІВ OSINT-РОЗВІДКИ»

Виконав: студент групи KN1-M22
спеціальності 122 Комп’ютерні науки
Рисюк Аспазій Вадимович

Керівник: **Смалько О.А,** доцент
кафедри комп’ютерних наук,
кандидат педагогічних наук, доцент

Рецензенти:
Оптасюк С.В, завідувач кафедри
фізики, кандидат фізико-
математичних наук, доцент;
Фурман І.Г., старший викладач
кафедри археології, спеціальних
історичних і правознавчих
дисциплін, кандидат юридичних наук

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

Актуальність дослідження полягає в тому, що на сьогоднішній день практично немає людини, яка б не користувалася соціальними мережами, багато злочинів, які скоюються в сучасному світі, плануються саме в інтернет-просторі, через спілкування в месенджерах, шляхом надсилання фото з зашифрованим місцем скоєння злочину тощо. OSINT-розвідка здатна ефективно протидіяти злочинам, які скоюються в кіберпросторі. Єдиною передумовою є те, що методику цю слід використовувати з урахуванням міжнародного досвіду. Одним з методів збору оперативної інформації є застосування засобів розвідувального аналізу відкритих джерел. Збільшення зацікавленості в OSINT-розвідки на сьогоднішній день спостерігається не лише з боку журналістів, аналітиків приватних компаній та пересічних громадян, але й з боку аналітиків спецслужб, оскільки ця система має певні переваги перед збором, опрацюванням та аналізом інформації з обмеженим доступом, причому насамперед у тому, що не вимагає спеціального доступу до інформації, а значить заощаджує час користувачу, а також не вимагає спеціальних навичок та істотних капіталовкладень. Використання засобів «OSINT» у деяких випадках дає змогу запобігти скоєнню злочинну, адже вислів «Краще попередити злочин, ніж за нього карати» набуває все більшого значення.

Об'єктом дослідження є сфери застосування технології OSINT-розвідки.

Предметом дослідження є методи та програмні інструменти добування корисної інформації з відкритих онлайн-джерел.

Метою кваліфікаційної роботи є дослідження засобів пошуку та аналізу інформаційних ресурсів з відкритих онлайн-джерел, вивчення можливостей їхнього оптимального застосування, а також визначення перспектив розвитку OSINT-технологій у майбутньому.

Завдання дослідження:

1. Вивчення ключових понять та принципів OSINT-технології.
2. Опис основних сфер застосування OSINT- технології.

3. Визначення технічних, програмних та інформаційних ресурсів, що використовуються у сфері OSINT.
4. Аналіз ефективності методів та інструментів для збору відкритої інформації.
5. Проектування та розробка системи, що дозволяє ефективно аналізувати та класифікувати результати пошуку відповідно до визначених критеріїв.

Методи дослідження включають в себе: вивчення наукових публікацій та літератури, що стосується добування інформації з відкритих джерел та методів OSINT-розвідки, порівняння та оцінка ефективності інструментів, використовуваних для збору та опрацювання інформації з відкритих джерел, опрацювання та аналіз отриманих в ході дослідження статистичних даних з метою визначення ефективності застосування технології, розгляд практичних прикладів застосування технології з метою добування конкретної інформації з відкритих джерел.

Робота складається з вступу, трьох розділів, списку використаних джерел, висновків і п’ятьох додатків.

Апробацію результатів дослідження здійснено у вигляді тез доповіді у збірнику матеріалів наукової конференції здобувачів вищої освіти фізико-математичного факультету Кам’янець-Подільського національного університету імені Івана Огієнка (1 листопада 2023 року) [1].

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було досягнуто мету- досліджено різноманітні засоби пошуку та аналізу інформаційних ресурсів з відкритих онлайн-джерел, вивчено можливості їхнього оптимального застосування, а також визначення перспектив розвитку OSINT-технологій у майбутньому. Виконано всі завдання дослідження, а саме:

1. Вивчено основні поняття та принципи OSINT-технології.
2. Проаналізовано основні сфери застосування OSINT- технології.
3. Досліджено різноманіття технічних, програмних та інформаційних ресурсів, що використовуються у сфері OSINT.
4. Проаналізовано ефективність багатьох методів та інструментів для збору відкритої інформації.
5. Спроектовано та розроблено систему, що дозволяє ефективно аналізувати та класифікувати результати пошуку відповідно до визначених критеріїв.

В ході та за підсумками виконання цієї кваліфікаційної роботи мною були зроблені такі висновки: результати дослідження підтверджують, що OSINT є ключовою складовою розвідки, забезпечуючи безпеку та ефективні розвідувальні заходи через використання публічної інформації; основні методи та інструменти OSINT призначені для отримання об'єктивних та релевантних даних.

Вивчення ключових елементів з використанням публічної інформації є стратегічно важливою частиною розвідувального процесу, що забезпечує глибоке розуміння ситуації та прийняття обґрунтованих рішень. Важливість дотримання етичних та правових норм під час застосування методів OSINT підкреслюється для забезпечення легітимності діяльності.

Розширення сфери застосування OSINT-розвідки ґрунтується на її універсальності в умовах аналізу кібербезпеки та вирішення геополітичних конфліктів, забезпечуючи високий рівень інформаційної обізнаності. Результати

дослідження методологій роботи в галузі OSINT підкреслюють необхідність систематизації та ефективного використання відкритих джерел інформації.

Структурований підхід до збору та аналізу даних дозволяє OSINT-розвідникам досягати точних та комплексних результатів. Використання методологій, що враховують етичні та правові аспекти, підвищує професіоналізм в сфері OSINT та забезпечує відповідність законодавству. Аналіз програмних інструментів у галузі OSINT підтверджує вагомий внесок технологій у вдосконалення розвідувальних процесів. Використання інструментів, таких як аналітичні платформи, веб-скрапінг та аналіз соціальних мереж, розширює можливості отримання інформації.

Оптимальний вибір та комбінація програмних засобів дозволяють забезпечити високу швидкість та точність обробки даних, а також підвищити ефективність розвідувальних операцій в цифровому середовищі.

Для створення системи інформаційного пошуку використовувались наступні інструменти: об’єктноорієнтована мова програмування C++, середовище розробки Qt Creator, СУБД Neo4j, пошукова система Elasticsearch, фреймворк Graphaware, високорівнева мова програмування Python та парсер Beautifulsoup. Розроблено архітектуру програмного продукту, який складається з 6 модулів: модуль збору даних, модуль відправки даних до БД, модуль інтерфейсу, модуль синхронізації БД, графова база даних, пошукова система. Впроваджено нереляційну базу даних, що зберігає інформацію у вигляді семантичної мережі. Порівнюючи із системами Hakia та Kosmix, слід відзначити, що створена система, хоча не має такого обширного функціоналу, пропонує зрозумілий інтерфейс та відсутність реклами.

Розроблений продукт може бути корисним інструментом для інформаційної розвідки, допомагаючи знаходити та зберігати надійні джерела інформації в інтернеті. Використання його як пошукової системи, при умові наявності потрібних даних у базі, може сприяти ефективному інформаційному пошуку. Таким чином, розроблений продукт є актуальним та може бути впроваджений на практиці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Рисюк А. Дослідження технології добування корисної інформації з відкритих онлайн-джерел. Збірник матеріалів наукової конференції здобувачів вищої освіти фізико-математичного факультету Кам'янець-Подільського національного університету імені Івана Огієнка. 1.11.2023 року. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С. 40. URL: http://elar.kpnu.edu.ua/xmlui/handle/123456789/7648

2 Andrews RJ. Info We Trust: How to Inspire the World with Data. Wiley. 2019. 272p.

3 A Beginner's Guide to OSINT Investigation with Maltego. URL: https://wondersmithrae.medium.com/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc

4 A Guide To Open Source Intelligence. URL: https://itsec.group/blog-post-osint-guide-part-1.html

5 Academy of cyber technologies of Ukraine. OSINT. Сучасна кіберрозвідка. URL: https://www.youtube.com/watch?v=Qjal2T3lOSU

6 BSides. URL: https://www.securitybsides.com/w/page/12194156/FrontPage

7 Bellingcat. URL: https://www.bellingcat.com

8 Bazzell M., Carroll J. The Complete Privacy & Security Desk Reference: Volume I: Digital. CreateSpace Independent Publishing Platform. 2016. 492 p.

9 Baker R. L. Deep Dive: Exploring the Real-world Value of Open Source Intelligence 1st Edition. Wiley, 2023. 544 p.

10 Brügger N., Schroeder R. Web as History: Using Web Archives to Understand the Past and the Present. UCL Press., Illustrated edition. 2017. 296 p.

11 Bazzell M. Open Source intelligence techniques: Resources for searching and analyzing online information Sixth Edition. Independently published, 2023. 550 p.

12 Bazzell M. Open Source Intelligence Techniques Resources for Searching and Analyzing Online Information. Independently published, 2021. 666 p.

13 Bellingcat’s Digital Toolkit. URL:https://archive.comsuregroup.com/wp-content/uploads/2018/06/Bellingcats-Digital-Toolkit.pdf

14 Blum I., Williams H. J. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Santa Monica: RAND Corporation, 2018. 62 p. URL: https://www.rand.org/pubs/research_reports/RR1964.html

15 Bielska A. Open source intelligence tools and resources handbook. 2020. 510 p. URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

16 Everything about Open source intelligence and osint investigations. URL: https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations/

17 Cybernews Blog. URL: https://cybernews.com/blog/

18 COOK S. A Guide to Open-Source Intelligence (OSINT). URL: https://greydynamics.com/a-guide-to-open-source-intelligence-osint/

19 CQR OSINT. URL: https://cqr.company/pentesting-process/osint/

20 Додонов А.Г. Распознавание информационных операций/ А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. Киев: ООО «Инжиниринг», 2017. 282 с.

21 DEF CON. URL: https://www.defcon.org/

22 David Bombal. OSINT social media. URL: https://www.youtube.com/watch?v=F6l2Bmh7Dq4

23 David Bombal Clips. Where to start in OSINT? URL: https://www.youtube.com/watch?v=ALy5bUMUo7Q

24 Goyal S. Sublist3r – Fastest Subdomain Enumeration Tool. URL: https://secnhack.in/sublist3r-fastest-subdomain-enumeration-tool/

25 Maltego - Cyber Weapons Lab - Research like an OSINT Analyst. URL: https://www.youtube.com/watch?v=46st98FUf8s

26 McFarlane D. A Beginners Guide to OSINT. URL: https://www.csnp.org/post/a-beginners-guide-to-osint

27 Hackathon A. OSINT VM. URL: https://www.tracelabs.org/blog/osint-vm-august-hackathon

28 Hadnagy C. Social Engineering. John Wiley &Sons. 2010. 410 p.

29 Mitnick K. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Back Bay Books. 2012. 448 p.

30 Hassan N. A., Hijazi R. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence 1st ed. Edition. Apress, 2018. 377 p.

31 IntelTechniques. URL: https://inteltechniques.com/

32 Nicole Beckwith - Mind Hacks – Psychological profiling, and mental health in OSINT investigations. URL: https://www.youtube.com/watch?v=104WpJm_eGk

33 OSINT Curious. URL: https://docs.github.com/en/pages

34 OSINT — Beginner's Guide (Part 1). URL: https://medium.com/@Aardwarewolf/what-is-osint-part-1-91aaa3890643

35 Open Source INTelligence (OSINT) Reference Sheet. URL:https://tpia.com/resources/Pictures/2019%20CPE%20files/OSINT%20Resources.pdf

36 Python theHarvester – How to use it? URL: https://www.geeksforgeeks.org/python-theharvester-how-to-use-it/

37 Open Source Intelligence Techniques (OSINT) for Fraud Prevention. URL: https://seon.io/resources/guides/open-source-intelligence-techniques-osint-for-fraud-prevention/

38 OSINT COMBINE. URL: https://www.osintcombine.com/training

39 OSINT Framework. URL: https://osintframework.com

40 OSINT-розвідка: як дії цивільних людей можуть допомагати ворогу? URL: https://www.youtube.com/watch?v=Gf3wgyykSjM&t=307s

41 OSINT-FR. OSINT Origins. URL: https://www.youtube.com/watch?v=XrTFzZ77eEI

42 OSINT TEAM. The Atypical OSINT. URL: https://osintteam.blog/the-atypical-osint-guide-2023-276a8d00959

43 OSINT Guide – Open Source Intelligence. URL: https://www.osintguide.com

44 Picolet J. Operator Handbook: Red Team + OSINT + Blue Team Reference. Independently published, 2020. 312 p.

45 Top OSINT. URL: https://www.maltego.com/blog/top-osint-infosec-resources-for-you-and-your-team/

46 SANS Cyber Security Webinars. URL: https://www.sans.org/webcasts/

47 SANS Cyber Defense. Lessons Learned from Ten Years of OSINT Automation. URL: https://www.youtube.com/watch?v=SMGEhFXURzY

48 SpiderFoot HX. URL: https://cybermarket.com.ua/product/spiderfoot-hx/

49 Trace Labs Blog. URL: https://www.tracelabs.org/blog

50 Trace Labs. Trace Labs OSINT VM – A Brief Tour. URL: https://www.youtube.com/watch?v=FlGdSZk1F6o&pp=ygUQVHJhY2UgTGFicyBvc2ludA%3D%3D

51 Trace Labs. Trace Labs - Open Source Intelligence Gathering. URL: https://www.youtube.com/watch?v=oz26mOwsse0&list=PL5ylEZWzbUEDsKTKdHrUVkAw0ZPqHzuj0

52 The Ultimate Beginner's Guide to OSINT. URL: https://www.osint-jobs.com/post/the-ultimate-beginners-guide-to-osint

53 The Ultimate Guide to the OSINT framework. URL: https://x-ray.contact/blog/the-ultimate-guide-to-the-osint-framework/

54 The Cyber Mentor. Open-Source Intelligence (OSINT). URL: https://www.youtube.com/watch?v=qwA6MmbeGNo

55 The OSINT Cycle: Getting familiar with the process of data collection and analysis. URL: https://osintteam.blog/the-osint-cycle-getting-familiar-with-the-process-of-data-collection-and-analysis-day3-of-6f53fcdb4234

56 Troia V. Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques 1st Edition. Wiley, 2020. 544 p.

57 Udemy. URL: https://www.udemy.com/

58 Layton R., Watters P.A. Automating Open Source Intelligence: Algorithms for OSINT. Syngress. 2015. 222 p.

59 Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. Wiley. 2003. 368 p.

60 OSINT 2021 guide: tools and techniques for threat intelligence. URL: https://www.authentic8.com/blog/OSINT-2021-guide-tools-and-techniques

61 Open Source Intelligence (OSINT) Guide. URL: https://www.eweek.com/big-data-and-analytics/open-source-intelligence-osint/

62 A Guide to Open Source Intelligence. URL: https://www.cjr.org/tow_center_reports/guide-to-osint-and-hostile-communities.php

63 Virtual machines for OSINT. URL: https://www.learnallthethings.net