УДК 343.85:004(477)
DOI https://doi.org/10.32850/sulj.2024.4.7

OSINT В КОНТЕКСТІ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ

Демедюк С. В.

У статті акцентовано на важливості використання систем та методів OSINT у протидії кіберзлочинності. Кіберзлочинність визначається як будь-яка незаконна діяльність, пов'язана з одним або кількома компонентами Інтернету, такими як веб-сайти, чати або електронна пошта. Зазначено що виділяється три різні типи кіберзлочинності: традиційні форми злочинів з використанням кіберпростору, незаконним контентом, і злочинами, характерними для електронних мереж.

Водночас акцентовано увагу і на кібератаках як надзвичайній кіберзагрозі. Такі атаки порушують легітимну роботу мережі і включають навмисне нанесення шкоди мережевим пристроям, перевантаження мережі та відмову в наданні послуг легітимним користувачам. Виділено та охарактеризовано два типи кібер атак: цілеспрямовані та ситуаційні.

Зазначено, що для протидії кіберзлочинності, особливо в організованих формах, здатності діяти віддалено через облікові записи, які неможливо відстежити, а також для боротьби з онлайн-злочинними угрупованнями важливо забезпечити правоохоронні органи та суб'єктів національної безпеки інструментами для виявлення, класифікації та захисту від різних типів кібератак та злочинів. Сучасні тренди злочинності, зокрема й у кіберпросторі, прискорюють використання відкритих джерел в Інтернеті для виявлення та запобігання кіберзлочинам, допомагають у формуванні більшої обізнаності щодо цілісної картини кіберзлочинності, злочинців та їх діяльності.

Зазначено, що методи використання відкритих джерел включають низку спеціальних дисциплін, зокрема статистику, data mining, машинне навчання, нейронні мережі, аналіз соціальних мереж, обробку сигналів, розпізнавання шаблонів (моделей), методи оптимізації та підходи до візуалізації. Наводяться різноманітні ініціативи фахівців та вчених щодо використання нових методів та технологій збору та анлізу даних з відкритих джерел для розслідування кіберзлочинів.

Порівнюючи різні аспекти методів, запропоновано класифікацію методів та моделей розслідування кіберзлочинів.

Ключові слова: *Open Source Intelligence, OSINT, кіберзлочинність, кібератаки, розслідування, методи.*

Demediuk S. V. OSINT in the context of cybercrime detection and prevention

The article emphasizes the importance of using OSINT systems and methods in countering cybercrime. Cybercrime is defined as any illegal activity related to one or more components of the Internet, such as websites, chat rooms, or e-mail. It is noted that there are three different types of cybercrime: traditional forms of crime using cyberspace, illegal content, and crimes specific to electronic networks.

At the same time, attention is also focused on cyberattacks as an extreme cyber threat. Such attacks disrupt the legitimate operation of the network and include intentional damage to network devices, network overload, and denial of services to legitimate users. Two types of cyber attacks are identified and characterized: targeted and situational.

It is noted that in order to counteract cybercrime, especially in its organized forms, the ability to act remotely through untraceable accounts, and to combat online criminal groups, it is important to provide law enforcement agencies and national security entities with tools to detect, classify and protect against various types of cyberattacks and crimes. Current trends in crime, including in cyberspace, accelerate the use of open sources on the Internet to detect and prevent cybercrime, and help to create greater awareness of the holistic picture of cybercrime, criminals and their activities.

It is noted that the methods of using open sources include a number of special disciplines, including statistics, data mining, machine learning, neural networks, social network analysis, signal processing, pattern recognition, optimization methods and visualization approaches. Various initiatives of specialists and scientists to use new methods and technologies for collecting and analyzing data from open sources to investigate cybercrime are presented.

Comparing various aspects of the methods, the author proposes a classification of methods and models for investigating cybercrime.

Key words: *Open Source Intelligence, OSINT, cybercrime, cyberattacks, investigation, methods.*

Постановка проблеми. Вплив кіберзлочинності змусив розвідувальні та правоохоронні органи по всьому світу розвивати сучасні методи та інструменти боротьби зі злочинністю. У цьому контексті важливим є використання OSINT, оскільки кількість доступних відкритих джерел стрімко зростає, і протидія кіберзлочинності все більше залежить від передових програмних засобів та методів збору й обробки інформації в ефективний і результативний спосіб.

Метою статті є системний аналіз кіберзлочинності та представлення OSINT інструментарію в контексті кібербезпеки та протидії кіберзлочинності.

Виклад основного матеріалу. Розглядаючи питання пов'язані з протидією кіберзлочинності, фахівцями та представниками різних фахових груп використовуються різні та взаємопов'язані терміни у зазначеному контексті діяльності, зокрема: «комп'ютерна злочинність», «інтернет-злочинність», «онлайн-злочинність», «високотехнологічні злочини», «злочини у сфері інформаційних технологій» та «кіберзлочини». У загальному значенні кіберзлочин – це будь-яка незаконна діяльність, пов'язана з одним або кількома компонентами Інтернету, такими як веб-сайти, чати або електронна пошта [1], і зазвичай визначається як «кримінальне правопорушення, вчинене з використанням Інтернету або іншої комп'ютерної мережі як компонента злочину» [2]. У 2007 році Європейська комісія (ЄК) визначила три різні типи кіберзлочинності: традиційні форми злочинів з використанням кіберпростору, пов'язані, наприклад, з підробкою документів, шахрайством в інтернет-магазинах і на електронних ринках, незаконним контентом, таким як дитяча порнографія, і «злочинами, характерними для електронних мереж» (наприклад, хакерство і атаки типу «відмова в обслуговуванні»). Автори публікації [3] розрізняють «справжню» кіберзлочинність (тобто нечесні або зловмисні дії, які не існували б поза межами онлайнового середовища) від злочинів, які є просто «електронними». Вони представили «справжні» кіберзлочини як хакерство, розповсюдження вірусів, кібервандалізм, викрадення доменних імен, DoS/DDoS атаки, на відміну від «електронних» злочинів, таких як зловживання кредитними картками, крадіжка інформації, наклеп, чорна розсилка, кіберпорнографія, сайти ненависті, відмивання коштів, порушення авторських прав, кібертероризм і шифрування. Водночас, фахівцями сьогодні зазначається, що злочинність проникла у Веб 2.0 «разом з усіма іншими видами людської діяльності» [3].

Кібератаки все частіше розглядаються як надзвичайна загроза національній безпеці. Такі атаки порушують легітимну роботу мережі і включають навмисне нанесення шкоди мережевим пристроям, перевантаження мережі та відмову в наданні послуг легітимним користувачам. Зловмисник також може використовувати зацикленість, помилки та неправильні конфігурації в програмному забезпеченні, щоб порушити нормальну роботу мережі [5].

Мета зловмисника – провести розвідку, обмеживши можливості вільно доступної інформації, отриманої за допомогою різних способів збору розвідувальних даних, перед тим, як здійснити цільову атаку [6]. Тим часом, «секретність» є ключовою частиною будь-якої організованої кібератаки. Дії можуть бути приховані за маскою анонімності, починаючи від використання всюдисущих кіберкафе і закінчуючи витонченими зусиллями з приховування інтернет-маршрутизації [1]. Кіберзлочинці використовують можливості анонімності та маскування під час спілкування в Інтернеті для здійснення шкідливих дій, таких як фішинг, спам, шантаж, крадіжка особистих даних і торгівля наркотиками [7; 8]. Інструменти мережевої безпеки допомагають розпізнавати вразливості мережі та збирати статистику сайтів. Мережеві зловмисники намагаються виявити проломи в безпеці на основі загальних служб, відкритих на хості, збираючи відповідну інформацію для запуску успішної атаки.

Автор публікації [9] класифікував кібератаки на два типи: цілеспрямовані та ситуаційні. При цілеспрямованих атаках застосовуються специфічні інструменти проти конкретних кібер-цілей, що робить цей тип більш небезпечним, ніж інший. Ситуаційні атаки спричиняють розповсюдження хробаків і вірусів, які розгортаються в Інтернеті без розбору [5].

Для протидії здатності організованої кіберзлочинності діяти віддалено через облікові записи, які неможливо відстежити, а також для боротьби з онлайн-злочинними угрупованнями важливо забезпечити правоохоронні органи та суб'єктів національної безпеки інструментами для виявлення, класифікації та захисту від різних типів атак [10]. Збільшення кількості і типів викликів для сучасних фахівців з національної безпеки, розвідки, правоохоронних органів і служб безпеки прискорило використання відкритих джерел в Інтернеті, щоб допомогти скласти більш цілісну картину про людей, організації та діяльність [11].

Методи використання відкритих джерел включають низку спеціальних дисциплін, зокрема

статистику, data mining, машинне навчання, нейронні мережі, аналіз соціальних мереж, обробку сигналів, розпізнавання шаблонів (моделей), методи оптимізації та підходи до візуалізації [12; 13].

Готтшальк та ін. [7] представили чотирьохетапну модель «Пошуку знань» для підтримки розслідувань і запобігання білокомірцевим злочинам в бізнесі [14]. Виділено чотири етапи:

- від слідчого до технології;
– від слідчого до слідчого;
– від слідчого до інформації;
– від слідчого до заяви.

Завдяки належному застосуванню знань такі процеси можуть допомогти у вирішенні проблем. Ця система, що складається з чотирьох частин, намагається зосереджувати увагу на підтримці пошуку доказів. У правоохоронних органах це важлива функція системи, оскільки докази визначають, чи буде особа звинувачена у вчиненні злочину [7], і наскільки успішним буде судовий розгляд.

Лінделауф та ін. [15] досліджували структурну побудову таємних злочинних мереж, використовуючи характеристику компромісу між секретністю та інформаційними можливостями для виявлення топологій злочинних мереж. Вони застосували цю методику до доказів у розслідуванні вибуху на Балі, здійсненого Джемаа Ісламією, а також до мереж розповсюдження героїну в Нью-Йорку. Дановскі [16] розробив методологію, що поєднує аналіз текстів і аналіз соціальних мереж, для пошуку осіб на дискусійних форумах, які мають дуже схожі семантичні мережі на основі змісту повідомлень, що спостерігаються членами списку спостереження, або на основі інших стандартів, таких як радикальний зміст, витягнутий з повідомлень, які вони поширюють в Інтернеті. У сфері протидії кібертероризму та підбурюванню до насильства Дановскі використовував пакистанський дискусійний форум з різноманітним контентом для отримання розвідувальної інформації про протиправну поведінку. Ігбал та ін. [17] представили уніфіковане рішення з data mining для вирішення проблеми аналізу авторства в анонімних текстових повідомленнях, таких як спам і поширення шкідливого програмного забезпечення, а також для моделювання стилю письма підозрюваних в контексті кіберзлочинної поведінки.

Брантінгем [18] запропонував комплексну обчислювальну систему для мережевого аналізу даних про спільні злочини, яка поєднує формальне моделювання даних з аналізом великих масивів даних про злочинність і тероризм, спрямований на виявлення спільних та актуальних шаблонів. Петерсен та ін. [19] запропонували алгоритм видалення вузлів в контексті кібертероризму для видалення ключових вузлів терористичної мережі. Фаллах [20] запропонував стратегію на основі теорії ігор з використанням концепції рівноваги Неша (Nash Equilibrium) для обробки складних сценаріїв DoS-атак. Чонка та ін. [21] запропонували рішення за допомогою Cloud TraceBack (CTB) для пошуку джерела DoS-атак і запровадили використання мережі з нейтральним зворотним поширенням, яка отримала назву «Cloud Protector», яка була навчена виявляти та фільтрувати трафік таких атак. Автори публікації [22] запропонували використовувати систему байєсівського переконання для оцінювання ризиків та кількісного визначення кібер-ризиків та кібер-вразливостей (CVA).

Наявні на сьогоднішній день методи можна класифікувати за схемою, як показано на рис. 1. Перший рівень загальних напрямів формується на основі напрямів: аналіз соціальних мереж, Data Mining та статистичного аналізу. Аналіз соціальних мереж передбачає використання таких методів: видалення вузла, вилучення мережі та семантичний аналіз мережі. У свою чергу Data Mining формується чотирма напрямами: текс-майнінг, оптимізаційний метод, веб-майнінг та магинне навчання. Ключовим же напрямом статистичного аналізу залишається регресійний метод.

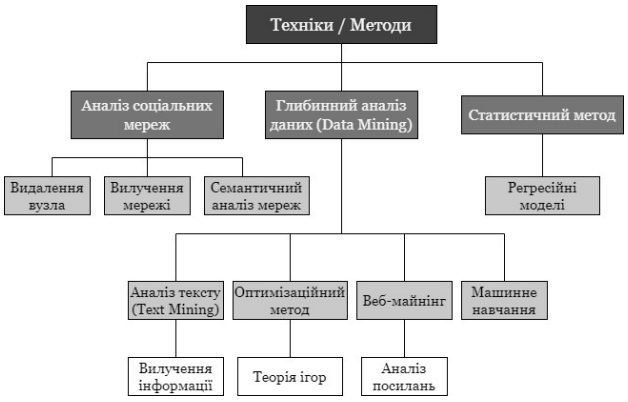

Рис. 1. Класифікація методів та моделей розслідування кіберзлочинів

Таким чином, сфера комп'ютерної кримінології включає в себе широкий спектр обчислювальних методів для ідентифікації:

– шаблонів і появи трендів;
– причини та умови злочинності;
– соціальних та просторових мереж тероризму, організованої злочинності та банд;
– мереж співучасників злочинів.

Висновки. Хоча багато підходів здаються корисними для розслідування кіберзлочинів, існуюча література свідчить про те, що аналіз соціальних мереж, інтелектуальний аналіз даних, аналіз текстів, кореляційні дослідження та методи оптимізації, особливо з акцентом на аналізі великих обсягів даних з відкритих джерел, є найбільш практичними методами, які допоможуть практикам, службам безпеки та судово-експертним установам.

Література

1. Govil J., Govil J. Ramifications of cyber crime and suggestive preventive measures. *Electro/information technology*. Chicago: IEEE, 2007. С. 610–615. DOI:10.1109/EIT.2007.4374526.

2. Agarwal V.K., Garg S.K., Kapil M., Sinha D. Cyber crime investigations in India: rendering knowledge from the past to address the future. *ICT and critical infrastructure: proceedings of the 48th annual convention of CSI, vol. 2*. Springer International Publishing Switzerland, 2014. С. 593–600. DOI:10.1007/978-3-319-03095-1_64.

3. Burden K., Palmer C. Internet crime: cyber crime – A new breed of criminal? *Computer Law & Security Review*. 2003. *Vol. 19*, no. 3. С. 222–227.

4. Hobbs Ch., Morgan M., Salisbury D. *Open source intelligence in the twenty-first century*. Palgrave, 2014. С. 1–6.

5. Hoque N., Bhuyan H., Baishya R.C., Bhattacharyya D.K., Kalita J.K.V. Network attacks: taxonomy, tools and systems. *Journal of Network and Computer Applications*. 2014. *Vol. 40*. С. 307–324. DOI:10.1016/j.jnca.2013.08.001.

6. Enbody R., Soodo A. *Intelligence gathering*. Elsevier, Targeted cyber attacks, 2014. ISBN 9780128006047.

7. Gottschalk P., Filstad C., Glomseth R., Solli-Sæther H. Information management for investigation and prevention of white-collar crime. *International Journal of Information Management*. 2011. *Vol. 31*. С. 226–233.

8. Igbal F., Fung B.C.M., Debbabi M. Mining criminal networks from chat log. *2012 IEEE/WIC/ACM international conferences on web intelligence and intelligent agent technology*. Macau: IEEE, 2012. С. 332–337. DOI:10.1109/WI-IAT.2012.68.

9. Kshetri N. Pattern of global cyber war and crime: a conceptual framework. *International Journal of Information Management*. 2005. *Vol. 11*. С. 541–562.

10. Simmons C., Ellis C., Shiva S., Dasgupta D., Wu Q. AVOIDIT: a cyber attack taxonomy. *Annual symposium on information assurance*. Office of Naval Research (ONR), 2014.

11. Appe E.J. *Behavior and technology, Internet Searches for Vetting, Investigations, and Open-Source Intelligence*. Taylor and Francis Group, 2011. С. 3–17.

12. Chen L.P., Zhang C.Y. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Science*. 2014. С. 314–347.

13. Akhgar B., Bayerl S. P., Sampson F. (Ed.). *Open Source Intelligence. Investigation. From Strategy to Implementation*. Advanced Sciences and Technologies for Security Applications. Springer International Publishing AG, 2016.

14. Gottschalk P. *White-collar crime: detection, prevention and strategy in business enterprises*. Boca Raton, Florida, USA: Universal-Publishers, 2010. ISBN-10: 1599428393, ISBN-13: 9781599428390.

15. Lindelauf R., Borm P., Hamers H. Understanding terrorist network topologies and their resilience against disruption. *Counterterrorism and open source intelligence* / Ed. Kock Wiil U. Vienna: Springer, 2011. С. 61–72. DOI:10.1007/978-3-7091-0388-3_5.

16. Danowski J.A. Counterterrorism mining for individuals semantically similar to watchlist members. *Counterterrorism and open source intelligence* / Ed. Kock Wiil U. Berlin: Springer, 2011. С. 223–247. DOI:10.1007/978-3-7091-0388-3_12.

17. Iqbal F., Binsalleeh H., Fung B.C.M., Debbabi M. A unified data mining solution for authorship analysis in anonymous textual communications. *Information Science*. 2013. *Vol. 231*. С. 98–112.

18. Brantingham P.L. Computational criminology. *2011 European intelligence and security informatics conference*. IEEE Computer Society, 2011. DOI:10.1109/EISIC.2011.79.

19. Petersen R.R., Rhodes C.J., Kock Wiil U. Node removal in criminal networks. *2011 European intelligence and security informatics conference*. IEEE Computer Society, 2011. С. 360–365.

20. Fallah M. A puzzle-based defence strategy against flooding attacks using game theory. *IEEE Transactions on Dependable and Secure Computing*. 2010. *Vol. 7*. С. 5–19.

21. Chonka A., Xiang Y., Zhou W., Bonti A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*. 2011. *Vol. 34*. С. 1097–1107.

22. Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., Sadhukhan S.K. Cyber-risk decision models: To insure IT or not? *International Journal of Decision Support Systems*. 2013. *Vol. 56*. С. 11–26. URL: http://dx.doi.org/10.1016/j.dss.2013.04.004.

Демедюк С. В.,
кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України