УДК 004.056
М. Серватнюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ МЕТОДІВ OSINT В СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ РИЗИКАМИ

UDC 004.056
M. Servatniuk

INTEGRATION OF OSINT METHODS INTO THE INFORMATION RISK MANAGEMENT SYSTEM

В сучасних умовах розвитку інформаційних технологій та всесвітньою мережі Інтернет постає питання здійснення ефективного пошуку інформації. Одним з таких засобів пошуку інформації є розвідка із відкритих джерел інформації (OSINT), яка являє собою концепцію, методологію і технологію пошуку та використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. [1]

У сферу інтересів OSINT входить пошук та аналіз відкритих баз даних, офіційних документів, комерційних та не комерційних ресурсів в і багато іншого. Таким чином систем OSINT дозволяє отримати відповідь на багато питань, що виникають, як у рядового користувача мережі Інтернет, так і в працівників сфери безпеки та спецслужб.

У теперішній час, за різними оцінками експертів, американські спецслужби отримують від 35% до 95% своїх розвідувальних даних із відкритих джерел. Частка витрат OSINT у розвідувальному бюджеті США складає лише 1% [2]. В Україні з 2014 р. робляться спроби використовувати OSINT у військових операціях, але застосування цього інструменту в державному управлінні та політиці захисту національних інтересів досі перебувають на стадії наукового пошуку [3].

Системи OSINT дає змогу систематизувати та узагальнити великі масиви інформації з відкритих джерел для проведення розгорнутого аналізу. Використовуючи інструменти OSINT, такі як Shodan, Google Dorks, Maltego, The Harvester, здійснювати пошук та аналіз інформації стає набагато швидше та простіше.

Веб-сайти та соціальні мережі можуть бути джерелом інформації, особливо про співробітників. Постачальники та партнери можуть також надавати доступ до певних деталей організації, які краще було б тримати в обмеженому доступі. Крім цього, існує велика кількість неіндексованих веб-сайтів та файлів, відомих під назвою «глибинна мережа», які залишаються технічно загальнодоступними.

Таким чином, при проведені ряду заходів, при перевірці інформації, яка знаходиться у вільному доступі за допомогою технологій OSINT можна запобігти витоку конференційної інформації.

Література.

1. Розвідка на основі відкритих джерел. URL: https://en.wikipedia.org/wiki/Open-source_intelligence.
2. Яровой Т. С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. URL: 18.pdf (maup.com.ua).
3. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. URL: https://www.rand.org/pubs/ research_reports/RR1964.html.