УДК 343.1:65.012.8+0043

Андрій Володимирович БІЛОБРОВ,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ

Отримання інформації у відкритих джерелах в інтересах розкриття і розслідування злочинів – одне з актуальних напрямків вдосконалення діяльності правоохоронних органів [1].

Діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору отримала назву OSINT – Open Source INTelligence (відкриті джерела розвідки). У сферу інтересів OSINT входить добування та аналіз офіційних документів, проектів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережевих щоденників і багато іншого.

Одним із різновидів інформаційних технологій збору та аналізу інформації з відкритих джерел є ще один напрямок розвідки – HUMINT (human intelligence), у дослівному перекладі - «розвідка по людям». До таких технологій відносяться: моніторинг соціальних мереж, опитування, соціальний інженірінг, залегендовані бесіди (під виглядом журналіста, клієнта, роботодавця тощо). У сучасному світі технології OSINT та HUMINT значно пов'язані між собою і використовують значну кількість технологічно подібних методів отримання необхідної інформації про об'єкт розвідки.

Важливим напрямком діяльності є зміцнення здатності розпізнавати внутрішні загрози у напрямку посилення вміння вживати ефективні дії для передбачення цих загроз та нейтралізації негативних явищ та процесів. Створення на національному рівні системи інтегрованої оцінки ситуації дасть можливість урухомити механізми моніторингу рівня реалізації стратегії та коригування її положень, з огляду на зміни у

безпековому середовищі. Ефективне реагування на динамічні політичні, економічні, соціальні та технологічні зміни є критерієм результативності системи внутрішньої безпеки з точки зору виявлення, ідентифікації та попередження загроз та джерел ризику. Це має теж прямий вплив на боротьбу зі злочинністю, зважаючи на врахування даних кримінальної розвідки при оцінці ситуації.

У правоохоронних органах західних держав існують спеціальні підрозділи, що здійснюють розвідку на основі відкритих джерел інформації. Наприклад, таку діяльність провадять: Scotland Yard OSINT, Royal Canadian Mounted Police OSINT, OSINT unit of New York Police Department, OSINT unit of the Los Angeles County Sheriff's Department, британська BBC Monitoring, ізраїльський Хатсав, австралійське Управління національних оцінок [2].

Відповідно до ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на власний розсуд. У межах кримінального провадження здійснення аналізу відкритих джерел інформації регламентовано главою 21 Кримінального процесуального кодексу України, зокрема в контексті розкриття порядку проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем.

Спеціальне програмне устаткування, таке як i2 Analyst`s Notebook, Maltego CE, надає можливість аналізувати соціальні мережі та визначати особливості взаємодії особи, яку підозрюють у вчиненні корупційного злочину, з іншими особами.

На початку цього року вийшов у світ черговий лінукс-дистрибутив для проведення кібер-розслідувань і OSINT під ім'ям CSI Linux Investigator. Даний дистрибутив містить програмне забезпечення, необхідне для вирішення наступних завдань: OSINT, Digital Forensics, Incident Response, Malware Analysis.

Ще одним відомим дистрибутивом є Maltegoю. Цей інтелектуальний інструмент для відстеження слідів кожного об'єкта в Інтернеті з відкритим вихідним кодом в основному використовується для виконання значних досліджень різних цілей за допомогою декількох вбудованих перетворень.

Також, популярності на даний момент набуває GitHub - нова Open Source бібліотека для OSINT, сервіс Hunter.io як інструмент пошуку адрес корпоративної пошти, за допомогою якого можна отримати кон-

тактну інформацію відповідно до домену. Такі відомості необхідні, щоб далі перевірити знайдені email на компрометацію. Hunter.io здатний обробити і витягти необхідні дані з 67 мільйонів відкритих джерел за допомогою 5 ключових методів: Domain Search - пошук email по домену або назвою організації; Email Finder - пошук окремого співробітника на ім'я і компанії; Email Verifier - підтвердження працездатності та актуальності пошти; Email Count - дозволяє дізнатися кількість email для одного домену або для однієї компанії; Account Information - управління особистим обліковим записом.

Застосування OSINT дозволяє отримати відповідь на багато питань, а також зосередити зусилля розвідувальних органів на виконання більш складних і «вузьких» завдань, не розпорошуючи сили інших напрямків розвідки на добування того, що можна отримати з відкритих джерел [3].

Таким чином, технологія OSINT є однією з важливих технологій різнорівневої різноформатної інформації, а також формування на її базі принципово нових знань. Поширення і використання перевіреної інформації з відкритих джерел дозволяє здійснювати обмін такою інформацією, оскільки при її отриманні не використовуються приховані методи і секретні джерела.

Ключовими факторами для успішного аналізу є: чітке розуміння цілей аналізу; неупередженість; збір інформації з максимально можливої кількості відкритих джерел; застосування коефіцієнтів ваги до кожної інформації; грамотний аналіз отриманої інформації.

Список бібліографічних посилань

1. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110–113.
2. Жарков Я. М., Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка*. 2013. Вип. 30. С. 38–41.
3. Молоков В. В. Эффективные способы получения открытой информации в сети интернет. *NovaUm.Ru*. 2017. № 9. С. 6–14.

Одержано 01.05.2020