Калиновський Олександр Валерійович, заступник начальника відділу організації науково-дослідної роботи Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник;
Школьніков Владислав Ігорович, здобувач вищої освіти ступеня «магістр» Національної академії внутрішніх справ

АНАЛІЗ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ КОРУПЦІЙНИХ ЗЛОЧИНІВ

На сучасному етапі розвитку суспільства розвиток високих технології призводить до перенасичення інформаційного поля людини. Станом на січень 2017 року близько 3,733 млрд населення світу користується можливостями Інтернету, 2,789 млрд – є активними користувачами соціальних мереж, 4,917 млрд – мають мобільні телефони [1].

Професор історії Єльського університету, аналітик ЦРУ Шерман Кент, відомий ще як «батько розвідувального аналізу», зауважив, що:

1) значну частину потрібної інформації можна отримати із відкритих джерел;

2) 90–95 % усіх даних відповідають дійсності.

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, с. 38].

Існують різні дефініції аналізу відкритих джерел інформації (англ. *OSINT*, або *Open source intelligence*). Так, Міністерство оборони США визначає поняття «аналіз відкритих джерел інформації» як процес своєчасного збору, використання, поширення загальнодоступної інформації для конкретного бенефіціара з метою вирішення розвідувальних задач. Із цього визначення можна виокремити ключову ознаку аналізу відкритих джерел інформації – збір інформації, яка є у відкритому доступі.

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, зокрема в контексті розкриття порядку проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем. Відповідно до ч. 2 ст. 264 Кримінального процесуального кодексу України *не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту* [3].

Здійснення такої негласної слідчої (розшукової) дії полягає в цілеспрямованому пошуку, зборі та фіксації інформації, що має значення для кримінального провадження, у мережах відкритої інформації, у тому числі Інтернету. На сучасному етапі наявність відкритих баз даних, існування соціальних мереж дає змогу отримувати інформацію щодо конкретних осіб, яких підозрюють у вчиненні корупційних злочинів, шляхом вивчення їхніх соціальних зв'язків, способу життя, здобуття персональних даних тощо. Це, відповідно, дає змогу слідчому, прокурору оперативніше вирішувати завдання кримінального провадження.

В Україні існує понад 150 баз даних, які є у відкритому доступі. Крім того, знання технік OSINT дає змогу отримувати додаткові відомості, які можуть стати корисними під час досудового розслідування.

Так, наприклад, до спеціальних технік OSINT належать:

– використання «логічних операторів» у різних пошукових системах мережі Інтернет;

– професійний пошук інформації в соціальних мережах Facebook, Twitter, Instagram, Linkedin тощо;

– ідентифікація осіб і місць за допомогою геолокації;

– пошук інформації в темних мережах (dark and deep web) тощо.

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. Крім того, Maltego CE є ефективним інструментом збору інформації (наприклад, адрес електронної пошти, номерів мобільного телефону особи тощо) в мережі Інтернет.

Водночас програма як The Harvester передбачає збирання адрес електронних пошт, піддоментів, хостів, імен працівників з різних публічних джерел мережі Інтернет.

FOCA (Fingerprinting Organizations with Collected Archives) – це інструмент, який використовується переважно для пошуку метаданих і прихованої інформації в документах, які вона сканує. Ці документи можуть бути на веб-сторінках, їх можна завантажити та проаналізувати за допомогою FOCA. Він здатний аналізувати широкий спектр документів, серед яких найбільш

поширеними є Microsoft Office, Open Office або PDF-файли, хоча він також аналізує, наприклад, файли Adobe InDesign або SVG.

Ці документи можна віднайти за допомогою трьох можливих пошукових систем: Google, Bing і DuckDuckGo. З усіма даними, отриманими із завантажених файлів, завдяки FOCA здійснюють ідентифікацію інформації, яка вказує, наприклад, на одну і ту саму команду розробників файлу, ідентифікацію серверів та клієнтів тощо.

Отже, OSINT – це ефективний інструмент збору інформації, який може бути застосований під час досудового розслідування корупційних злочинів. За допомогою цих технік слідчий зможе отримувати інформацію, яка матиме орієнтувальне значення.

Нині нагальною є потреба в законодавчому врегулюванні можливості використання такої інформації в кримінальному провадженні. Зокрема, слід внести зміни до чинного Кримінального процесуального кодексу України, які б стосувалися віднесення інформації в електронній (цифровій) формі до процесуальних джерел доказів, а також визначали б регламентацію використання сертифікованих програмно-апаратних засобів як умови визнання допустимості таких доказів.

Отже, з інформатизацією суспільства прозорість влади стає неминучим явищем, а тому контроль за діями органів державної влади за допомогою аналізу відкритих джерел інформації дає змогу не лише запобігати корупційним проявам, а й ефективно їх розслідувати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Strategic analysis, open source analysis, risk assessment and used analysis tools : матеріали тренінгу Консультативної місії Європейського Союзу (Київ, 15–19 трав. 2017 р.) ; Національна академія внутрішніх справ. – Київ, 2017.

2. Жарков Я. М. Наукові підходи щодо визначення суті розвідки з відкритих джерел / Я. М. Жарков, А. О. Васильєв // Вісник Київського національного університету імені Тараса Шевченка. – 2013. – Вип. 30. – С. 38–41. – (Серія «Військово-спеціальні науки»).

3. Кримінальний процесуальний кодекс України. – Київ : Паливода А. В., 2013. – 328 с.