

НАУКОВІ ДОПОВІДІ ПЕРЕМОЖЦІВ МІЖНАРОДНИХ І ВСЕУКРАЇНСЬКИХ СТУДЕНТСЬКИХ КОНКУРСІВ

Школьніков В. І., оперуповноважений
відділу оперативно-аналітичного
забезпечення управління захисту
економіки Департаменту захисту
економіки Національної поліції України

ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ АНАЛІЗУ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

Інформатизація суспільства зумовлює виникнення нових способів вчинення кримінальних правопорушень. Дедалі частіше правопорушники у своїй діяльності використовують можливості мережі Інтернет. Окремі проблеми в законодавчому регулюванні питання визнання допустимості доказів, які отримані безпосередньо з мережі Інтернет, підтверджують потребу в науковому дослідженні зазначеної проблематики та розробленні конкретних пропозицій щодо вдосконалення кримінально-процесуального законодавства.

Теоретичним і практичним розвідкам із цього питання були присвячені наукові праці таких учених: В. Д. Гавловського, Ю. М. Грошевого, Ю. Ю. Орлова, О. В. Капліної, В. Т. Нора, М. М. Панової, Д. І. Сапіги, С. М. Стахівського, А. В. Тарасюка, С. С. Чернявського, А. П. Шеремети й інших.

Існують різні дефініції аналізу відкритих джерел інформації (з англ. *open source intelligence*, OSINT). Так, Міністерство оборони США аналізом відкритих джерел інформації вважає процес своєчасного збору, використання, поширення загальнодоступної інформації для конкретного бенефіціара з метою вирішення розвідувальних задач. З цього визначення можна виокремити основну ознаку аналізу

відкритих джерел інформації – збір інформації, яка є у відкритому доступі.

На нашу думку, розкриваючи сутність технік аналізу відкритих джерел інформації, необхідно їх поділяти на такі різновиди (залежно від характеристик мережі Інтернет):

- техніки, які застосовують у поверхневих мережах;
- техніки, якими послуговуються в Даркнеті.

Техніки, які застосовують у поверхневих мережах, можна поділити на:

- професійне використання онлайн пошукових систем (використання можливостей інструменту «розширений пошук», кеш-пам'яті, логічних операторів, «підстановочних» операторів (англ. *wildcard operators*), використання пошукових систем для віднайдення веб-доменів, місцезнаходження IP тощо);

- пошук у двомовних пошукових системах (2lingual.com, yamli.com тощо);

- пошук фото- та відеофайлів (Google, Yahoo!, Bing, Exalead, Photobucket, SmugMug, Picasa, Stockxchng, Pixsy, YouTube, Truveo, DailyMotion, Metacafe, Vimeo, Spike, ClipBlast, Tineye, Zuula тощо);

- пошук на форумах і блогах;

- пошук номерів мобільних телефонів та адреси електронної пошти (Truecaller, Sync.me тощо);

- геопошук (GoogleMaps, BingMaps, GoogleEarth, Echosec, Welink, Geofeedia, Flightradar, Marinetraffic тощо);

- «архівний пошук» (онлайн-програма WayBackMachine дає змогу отримати інформацію, яка раніше містилася на конкретному веб-сайті);

- пошук у соціальних мережах (Facebook, Twitter, Google+, Wikipedia, LinkedIn, Reddit, Instagram, Myspace, YikYak, Pinterest, ресурси «Вконтакте» та «Однокласники» тощо).

На сьогодні результати аналізу відкритих джерел інформації не є доказами в кримінальному провадженні. У контексті питання щодо використання електронної інформації в

кримінальному судочинстві є достатньо врегульованим та навіть існують судові прецеденти визнання такої інформації доказами. Найбільшого успіху в цій сфері досягли Канада та США, де інформація із соціальних мереж, «скріншот» та інші подібні форми фіксації змісту веб-сайту визнають допустимими доказами в кримінальному судочинстві.

На нашу думку, для вирішення цього питання необхідно внести відповідні зміни до чинного КПК України, які передбачатимуть:

- визначення поняття «електронне відображення» та форми фіксації такої інформації (наприклад, портали, веб-сайти, електронні бази даних, файли тощо);

- зарахування електронного відображення до процесуальних доказів (ч. 2 ст. 84 КПК України);

- закріплення обов'язку збереження інтернет-провайдерів та операторів мобільного зв'язку електронного відображення на вимогу слідчого, прокурора в передбачених законодавством випадках;

- визначення обов'язку щодо проведення судових техніко-криміналістичних експертиз електронних відображень для встановлення відсутності факту підроблення такої інформації або джерела (веб-сайту, бази даних тощо), на яких така інформація містилася;

- закріплення в розділі IX КПК України «Міжнародне співробітництво під час кримінального провадження» права слідчого, прокурора направляти запити в онлайн-режимі до адміністрації соціальних мереж щодо отримання інформації про користувача такої мережі у випадках, пов'язаних із потенційною загрозою для дитини або небезпекою смерті чи серйозного фізичного ушкодження будь-якої особи.