Список бібліографічних посилань

1. Кустод А. М. Криминалистика и механихм преступления. Цикв лекцій. М. : Изд-во Моск. Психолого-социального института; Воронеж : Из-во НПО «МОДЭК», 2002. 304 с.
2. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. Інформаційні технології і засоби навчання. 2015. Том 49. № 5. С. 37-70.
3. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. В. Т. Бусел. К. ; Ірпінь : Перун, 2005. 1728 с.
4. Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. 480 с.
5. Положення про порядок ведення Єдиного реєстру досудових розслідувань : затв. наказом Генеральн. прокурора України від 17 серп. 2012 р., № 69. К., 2012.
6. Транснациональная организованная преступность: дефиниции и реальность: монография. Отв. ред. В. А. Номоконов. Владивосток. 2001. 375 с.
6. Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности: Монография. Харьков : Изд-во Нац. ун-та внутр. дел, 2002. 412 с.
7. Осипенко А. Л. Организованная преступность в сети Интернет. Вестник Воронежского Института МВД России. 2012. № 3. С. 10-15.

Одержано 23.10.2018

УДК 351.746.1(477)

Олег Борисович ФАРІОН,
кандидат військових наук, доцент,
професор кафедри управління оперативно-розшуковою діяльністю
факультету правоохоронної діяльності
Національної академії Державної прикордонної служби України ім.
Б. Хмельницького;
ORCID: https://orcid.org/0000-0001-6751-0468

ЩОДО ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ДЛЯ МОНІТОРИНГУ ТА ДОСЛІДЖЕННЯ ІНФОРМАЦІЇ З ПРИХОВАНИХ ІНТЕРНЕТ-РЕСУРСІВ ПРО ОЗНАКИ ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ

В сучасних умовах глобальної інформатизації та розвитку інформаційно-телекомунікаційних технологій суспільство отримало можливість масової комунікації та оперативного вирішення різних питань, зокрема й таких, які пов’язані з порушенням законодавства. Так, для організації та здійснення протиправної діяльності стали використовуватись більш досконалі способи та методи анонімного

спілкування та прихованого обміну інформацією (наприклад, організація «арабської весни»). Крім того, прогресивний розвиток Інтернету протягом останнього десятиріччя сприяв стрімкому поширенню злочинності та забезпечив її стійкість до превентивних заходів правоохоронних органів.

Одним із передових та ефективних інструментів, який використовується оперативно-розшуковими (далі – оперативними) підрозділами Державної прикордонної служби відповідно до наданих законодавством повноважень щодо протидії кримінальним правопорушенням, пов'язаним із торгівлею людьми, терористичною діяльністю та іншими злочинами, є кримінальний аналіз. Метою такого аналізу є пошук та фіксація ознак злочинної діяльності, встановлення та передбачення зв'язків між інформацією про злочини та іншими потенційно з ними пов'язаними даними, з використанням аналітичних методів, засобів та інформаційних ресурсів.

Інформація, яку можна отримати із різних інформаційних ресурсів, зокрема загальнодоступних сайтів Інтернету, наприклад, сайтів новин, є відкритою. Така інформація індексована пошуковими системами Google, Yahoo тощо. Тому пошук інформації про ознаки протиправної діяльності не викликає труднощів для кримінальних аналітиків оперативних підрозділів Державної прикордонної служби України.

Більш складнішим є моніторинг інформації, прихованої від загального користування. Така інформація у загальній своїй кількості є неіндексованою пошуковими системами та специфічною для отримання та аналізу. Тому в протиправній діяльності прихована інформація набула широкого розповсюдження та активно використовується. Обмін такого роду інформацією здійснюється за допомогою ресурсів прихованого, глибокого Інтернету («Deep Web») та спеціальних технологій «Dark Web» (наприклад, «Darknet», «TahoeLAFS», «Freenet»).

Відомо, що «Deep Web» є збіркою всіх неіндексованих сайтів Інтернету, до яких входять: бази даних користувачів, сторінки веб-пошти, сторінки, необхідні для реєстрації на веб-форумах та інше, що знаходиться поза можливостей відкритих пошукових сервісів Інтернету.

Одним із інструментів «Deep Web», який надає додаткові можливості, наприклад, спеціальні: автентифікацію, проксі-сервер, програмне забезпечення щодо отримання доступу до прихованої інформації є «Dark Web» (наприклад, «Шовковий шлях» щодо торгівлі рекреаційними препаратами).

Доступ до «Dark Web» здійснюється за допомогою спеціальних засобів, таких як «Tor», «I2P», «Freenet», «Manet», «NETSUKUKU» та інших. Для анонімного обміну інформацією щодо протиправної діяльності використовуються приховані файлообмінні мережі, такі як «RShare» та інші.

Спеціальний програмний продукт «Tor» дозволяє приховувати місцезнаходження користувача Інтернетом та унеможливити його

ідентифікацію, приховати активність браузера. Це надає злочинцям можливість відкрито реалізовувати знаряддя та засоби вчинення злочинів; розробляти тактику та обмінюватись формами і методами протиправної діяльності. Доступ до такого роду прихованої інформації здійснюється на http://godnotaba...xyz/ через наступні площадки:

– *торгівельні* (наприклад, medusas6rqee6…onion, freerj4lgqdjjuk...onion; psyco42coib33…onion; narniaanwmvmt…onion);

– *фінансові* (наприклад, blockchainbdgp...onion; astarotyn5uilx…onion);

– *спілкування* (наприклад, 7lvd7fa5yfbdq...onion);

– *поштові* (наприклад, zsolxunfmbfuq...onion; scryptmaildni...onion; secmailw453j7...onion);

– *ботів* (наприклад, erlach6sjul4...onion; rekt5jo5nuuad...onion);

– *з хостингом ілюстрацій і файлів* (наприклад, pic2tor5xilwq...onion);

– *записок* (наприклад, cryptorffquol...onion; cryptex3m3o4v...onion);

– *картингу/хакінгу* (kickassugvgof...onion; darksell2cukn...onion та інші);

– *інших* (наприклад, zcashph5mxqjj...onion; grams7enufi7j...onion).

Для обміну прихованою інформацією більш широкого спектру в «Tor» через https://thehidden...org використовується каталог «Hidden WiKi».

Пошук прихованої в Інтернеті інформації про ознаки протиправної діяльності ускладнюється через обмеження технічних ресурсів серверів (баз даних, програмного забезпечення) щодо зберігання значної кількості веб-форм та різноманітних тем на форумах «Dark Web». Крім того, цей процес унеможливлюється через обмежений доступ до сервісів, що пов'язано з необхідністю володіти та вводити логін та пароль. Також багато сервісів неможливо знайти за допомогою відомих пошукових систем з причин того, що посилання на такі сервіси не публікуються відкрито та доступні виключно власникам веб-сайтів, хостингу, провайдерам і нетсталкерам (через спеціалізоване програмне забезпечення для сканування діапазонів IP-адресів і перевірку пов'язаних з ними ресурсами).

На озброєнні правоохоронних органах передових країн світу існує низка методик пошуку інформації з прихованих ресурсів (наприклад, рандомайзери посилань; перевірка файлів, завантажених на файлообмінники; пошук будь-яких відомостей щодо заданої тематики на відкритих ресурсах; аналіз даних на «дошках оголошень» тощо. Однак, актуальним і найбільш результативним залишається сканування діапазонів IP-адрес за допомогою спеціальних програм, основними з яких є:

– «Advanced IP scanner» – через віддалене управління RAdmin, дозволяє сканувати довільні діапазони, але з певною похибкою: не охоплює всі доступні дані. Отримана інформація обмежена FTP-серверами, відкритими файлами і тими портами, до яких можна підключитися через RAdmin;

– «NMAP» – дозволяє знаходити безліч даних, але призначений для точкового сканування;

– «NESKA» – дозволяє автоматично відсилати всі знайдені результати пошуку адресатові.

Наявні на оснащенні підрозділів кримінального аналізу Державної прикордонної служби України спеціальні програмно-технічні комплекси, а також можливості взаємодіючих правоохоронних органів, дозволяють здійснювати моніторинг прихованих ресурсів Інтернету та виявляти ознаки протиправної діяльності під час дотику прихованої інформації з відкритою. Крім того, здійснювати за реальним часом геолокацію осіб, причетних до злочинів, та аналізувати зв'язки між ними, протиправними подіями та обставинами скоєння злочинів.

Моніторинг прихованої інформації в процесі кримінального аналізу здійснюється відповідно до поставленої мети методом пошуку, спрямованого на виявлення маловідомих, малодоступних і відвідуваних об'єктів з їх можливим подальшим аналізом, систематизацією та зберіганням. З цією метою застосовуються методики пошуку відомої та невідомої інформації. За першою методикою здійснюється точковий пошук файлів та відомих їх характеристик (розширення тощо). За другою – пошук таких файлів, сайтів, сторінок, про характеристики та властивості яких немає ніякої інформації. Оскільки в процесі моніторингу прихованої інформації здійснюється збір будь-якої інформації про протиправну діяльність, то друга методика є основною, а перша – такою, що доповнює другу.

Разом із тим, отримання прихованої інформації щодо обігу електронних валют «Bitcoin», IP-адрес технічних засобів комунікації, електронних адрес та інших контактних даних ймовірних правопорушників може здійснюватись через адміністраторів закритих сайтів.

Перспективою в застосуванні кримінального аналізу оперативними підрозділами Державної прикордонної служби України є створення масивів даних на основі систематизації прихованої інформації про ознаки протиправної діяльність та встановлення її напрямків та об'єктів посягань.

Висновок. Таким чином, проаналізовано загальні питання отримання і використання інформації з прихованих ресурсів Інтернету та висвітлено окремі аспекти механізму її моніторингу та дослідження оперативними підрозділами Державної прикордонної служби України за допомогою кримінального аналізу.

У подальших наукових дослідженнях становить інтерес формування з використанням спеціального програмного забезпечення «портрету злочинця», виявлення правопорушників за допомогою кримінального аналізу сукупності «метаданих» за параметрами, які реєструються в мережі Інтернету (наприклад, зацікавленістю користувача Інтернету, участю у групах).

Одержано 29.10.2018