Список бібліографічних посилань

1. Оперативно-розшукова діяльність : навч. посіб. / Є. М. Моісеєв, О. М. Джужа, Д. Й. Никифорчук та ін. ; за заг. ред. О. М. Джужі. Київ : Прав. єдність, 2009. 310 с.

2. Василинчук В. І. Оперативно-розшукова профілактика злочинів у бюджетній сфері : монографія. Київ : ФОП Кандиба, 2013. 519 с.

3. Про оперативно-розшукову діяльність : закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.

Одержано 21.11.2017

УДК 343.321.3:303.717

Михайло Степанович КУЦІЙ,
старший викладач спеціальної кафедри
Національної академії Служби безпеки України

СТЕГАНОМЕТОДИ ПРОТИДІЇ ПРИВАТНОМУ СПІЛКУВАННЮ ТОРГІВЦІВ ЛЮДЬМИ

Сьогодні однією із специфічних ознак оперативно-розшукової характеристики злочинного явища, пов'язаного з продажем людини або здійсненням стосовно неї іншої незаконної угоди, стає використання організованою групою у приватному спілкуванні так званого стеганографічного перетворення (вбудовування інформації в певний об'єкт (далі – контейнер), який в Інтернеті відкрито передається одержувачу) [1]. В таких контейнерах зловмисники залишають «віртуальні відбитки» [2] системи команд електронної обчислювальної машини (гаджет), застосованої в ході обміну прихованими документами (цифрова фотокартка переміщеної через державний кордон особи, файли обстеження органів чи тканин потерпілого для їхньої трансплантації тощо). Здобуті «віртуальні сліди» разом з отриманими у встановленому законом порядку іншими документами важливі як докази використання жертви злочину з певною метою, визначеною диспозиціями відповідних статей кримінальних кодексів України та країн-партнерів. Подібні «відбитки» виявляються спільними зусиллями з іноземними партнерами, передусім, у ході проведення операцій з контрольованої поставки за відсутності прямих загроз життю та здоров'ю учасників протидії торгівлі людьми.

В оперативно-розшуковій діяльності (ОРД) із метою виявлення, попередження та припинення злочинів проти волі і гідності людини використовується інститут конфіденційного співробітництва (КС): негласні штатні та позаштатні працівники [3], а в науковій літературі – конфіденти.

Із зазначеною метою окремі з них можуть перебувати в транснаціональних організаціях торгівців людьми та здійснювати приватне спілкування у цьому кримінальному середовищі.

Законодавець визначає таке спілкування як передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу [4]. За змістом статті 258 Кримінального процесуального кодексу України, спілкування для його учасників буде приватним, якщо відомості передаються та зберігаються за таких фізичних чи юридичних умов, при яких вони можуть розраховувати на захист інформації від втручання інших осіб. Для зловмисників такими сторонніми особами передусім є негласні працівники оперативних підрозділів.

Підстави та порядок втручання суб'єктів ОРД у приватне спілкування осіб, які обґрунтовано підозрюються в торгівлі людьми, передбачені чинним законодавством. Однак, зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) та електронних інформаційних систем (ст. 264 КПК) як негласні розшукові дії не завжди стають ефективними з точки зору здобування доказів у випадках, коли злочинці для передавання документів використовують новації стеганоперетворення, або роздільно розміщують частки одного файлу на різних потоках переміщення великих об'ємів контенту. Тому, на наш погляд, іноді важко переоцінити роль негласних працівників у виявленні гатжетів злочинців та встановленні місцезнаходження «віртуальних відбитків» використаних ними електронних засобів як доказів у кримінальному провадженні.

У ході контактів із транснаціональним криміналітетом завжди існує небезпека життю, здоров'ю, майну конфідентів та членів їхніх сімей від злочинних посягань. Передусім, унаслідок виникнення в зловмисників підозр щодо підтримання особою спілкування з оперативним підрозділом. При певних обставинах запобігання злочину проведення зустрічей з конфідентом взагалі неможливе. Однак, негласні штатні і позаштатні працівники зобов'язані зберегти таємницю, що стала їм відома під час КС, уникнути викриття та виконати завдання ОРД у відповідності з правовими нормами [5].

На нашу думку, ефективній протидії торгівцям людьми сприятиме використання правоохоронцями технологій комп'ютерної стеганографії, зокрема, впровадження у документи стеганографічних міток або стеганоміток (англ. stegomarks), які ідентичні лише для одного гаджету або його електронних файлів [6]. Оперативні працівники і конфіденти швидко навчаються використанню стеганоміток завдяки розповсюдженості в Інтернеті стеганопрограм та їхньої інтуїтивної зрозумілості.

Вже з початку двохтисячних років з практики відомі приклади використання зловмисниками в Україні стеганометодів для приватного спілкування. Наприклад, через мережу міських інтернет-кафе. З

міркувань особистої безпеки відправника у передаванні інформації застосовувався вихід на багатофункціональні, швидкі, масштабовані, розширювані та кешуючі сервери. Зокрема сервери, що обслуговують порно-сайти, тобто надають достатньо повну підтримку протоколу HTTP і дозволяють забезпечити як кешування статичних об'єктів, таких як файли, JavaScript, CSS і малюнки, так і виступати в ролі проміжної ланки, що перенаправляє запити до фронтенд-серверів, які генерують динамічний контент.

Прибувши до інтернет-кафе в обумовлений час така особа вже мала при собі цифровий об'єкт із вбудованим контейнером з інформацією, що зберігався, як правило, на гнучкому магнітному диску (т. зв. Floppy disk). Після передачі інформації магнітний носій одразу знищувався її відправником безпосередньо в кафе, тобто приміщення він залишав без речових доказів протиправної діяльності.

Таким чином, «відбиток пальцю» (fingerprint), «водяний знак» (watermark) та інші стеганометоди дозволяють з позицій кримінального середовища впроваджувати до цифрового об'єкту спеціальні мітки, які містить ідентифікаційні ознаки, що відомі лише його автору (наприклад, конфіденту) або оперативному підрозділу. За допомогою вбудованого ярлику легше відстежувати контент зловмисника та встановлювати місцезнаходження одержувача файлу.

На наш погляд, застосування стеганометодів у заходах оперативної закупки, контрольованої закупки та поставки відкривають нові можливості документування протиправних дій.

Наведемо лише один приклад. Якщо зловмисники прибігають до біткойну або іншої криптовалюти, то існує і можливість помітити її віртуальну матерію подібно нанесенню на паперовій банкноті люмінесцентного надпису «хабар». При цьому в правоохоронців немає потреби звертатися до банківської установи для виготовлення відповідного поміченого засобу.

З огляду на поширення використання у злочинній діяльності стеганометодів та інших новітніх технологій, оперативна практика постійно шукає доцільні рішення поєднання технічних новацій з апробованими прийомами та засобами протидії криміналу. Тому вважаємо, що в теорії ОРД застосовані в її інтересах стеганографічні програмні засоби доцільно відносити до несправжніх (імітаційних) та ідентифікованих (помічених) засобів.

Список бібліографічних посилань

1. Куцій М. С. Цифрова стеганографія для тайникових операцій в конфіденційному співробітництві. *Інформація і право*. 2016. № 1 (16). С. 124–131.

2. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М. : Горячая линия – Телеком, 2002. С. 144.

3. Про оперативно-розшукову діяльність : закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.

4. Кримінальний процесуальний кодекс України : наук.-практ. комент. : у 2 т. Т. 1 / Нац. акад. правових наук України ; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. 877 с.

5. Куцій М. С. Питання правового регулювання забезпечення зв'язку в конфіденційному співробітництві // Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності : тези Всеукр. наук.-практ. конф. Харків, 2017. С. 823–827.

6. *Хакер.* 2016. № 215. С. 9.

Одержано 17.11.2017

УДК 347.963(477)

Андрій Васильович ЛАПКІН,
кандидат юридичних наук, доцент,
доцент кафедри організації судових та правоохоронних органів
Національного юридичного університету імені Ярослава Мудрого

ДЕЯКІ ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОЧАТКОВОГО МОМЕНТУ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Згідно із ст. 214 Кримінального процесуального кодексу України (далі – КПК України), досудове розслідування розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР), що, в свою чергу, має відбутися невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення слідчим, прокурором з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення. Таким чином, законодавець пов'язує початок кримінального провадження (першою стадією якого є досудове розслідування) із моментом внесення відомостей до ЄРДР. Разом з тим, визначений у ст. 214 КПК України момент початку досудового розслідування викликає ряд запитань. Зокрема, про те, що слід вважати внесенням відомостей до ЄРДР, а також про те, який характер має діяльність, що передує такому внесенню.

Відповідь на це питання необхідно шукати у Положенні про порядок ведення Єдиного реєстру досудових розслідувань від 06.04.2016 (далі – Положення), згідно із п. 1 підрозділу 2 розділу II якого формування ЄРДР розпочинається з моменту внесення до нього Реєстратором (прокурором або слідчим) відповідних відомостей про кримінальне правопорушення, зазначених у заяві чи повідомленні про його вчинення або виявлених ним самостійно з будь-якого джерела. Разом з тим, п. 2 підрозділу 2 розділу II Положення передбачає здійснення керівником прокуратури, органу досудового розслідування