

вживання марихуани та інших наркотичних і сильнодіючих речовин, зроблені маркування «Тільки для вживання табаку!» або «Не для вживання заборонених речовин!». Іноді реалізують онлайн новітні сильнодіючі речовини, які ще не внесені до переліку заборонених, і перестають збувати їх одразу ж після законодавчої заборони.

5. Загальнодоступні сайти, призначені для спілкування, соціальні мережі де можуть обговорюватися різні питання щодо вживання наркотичних засобів.

6. Сайти створені, придбані або орендовані приватними особами, які використовують Інтернет з метою поширення у вільній формі своїх ідей про наркотики і про вживання наркотиків, а також з метою їх обговорення [2].

7. Сайти створені, придбані або орендовані приватними особами для здійснення рекламування та незаконного збуту наркотичних засобів та сильнодіючих речовин.

Окремо слід відзначити програмне забезпечення, яке є популярним для продажу заборонених речовин. Мова йде про інтернет-пейджери (наприклад, Skype, ICQ, Miranda, QIP) з анонімними акаунтами, через які здійснюється зв'язок покупця з продавцем. Найбільш розповсюджена схема реалізації наступна. Імена акаунтів або номери для зв'язку розміщуються на сторонніх сайтах або просто пишуться на стінах будівель у людних місцях. Вони нічого не скажуть сторонній людині, однак особи, що вживають наркотичні засоби за їх допомогою можуть легко зв'язатися з продавцем. Продавець приймає замовлення, оголошує ціну і номер банківської карти, на яку необхідно перерахувати гроші. Після перерахування грошей він робить «закладку» з наркотичним засобом, координати якої передає замовнику. Замовнику лишається тільки забрати «товар» із місця «закладки». Як видно, сама схема продажу не складна, однак вона значно ускладнює викриття навіть продавця, не говорячи про всю мережу, до якої входить конкретний продавець.

Враховуючи викладене вище, можна дійти висновку, що збут наркотичних засобів та сильнодіючих речовин з використанням мережі Інтернет є серйозним викликом для правоохоронних органів. Боротьба з даними видами злочину потребує постійного вивчення як нових способів і методів реалізації заборонених речовин та препаратів, так і можливостей Інтернет, які постійно розвиваються і удосконалюються і можуть бути використані із злочинною метою.

Список бібліографічних посилань: 1. Покровський А. Правоохоронні органи не контролюють продаж наркотиків через Інтернет // Волинь Post: сайт. URL: <http://www.volynpost.com/news/68105-pravoohoronni-organy-ne-kontrolyuyut-prodazh-narkotyktiv-cherez-internet-andrij-pokrovskij> (дада звернення: 01.10.2017). 2. Паутова Т. А. Выявление, документирование и расследование преступлений, связанных с незаконным оборотом наркотиков, в том числе с использованием электронных средств оплаты. *Концепт*. 2013. Т. 3. С. 1216–1220.

Одержано 03.10.2017

УДК 343.9

Олена Валеріївна ЛИННИК,

кандидат юридичних наук,

доцент кафедри кримінального процесу

та криміналістики Університету державної фіскальної служби України

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

В наш час, з метою прискорення обміну інформацією та підвищення ефективності праці, відбулося поєднання різноманітних інформаційних ресурсів глобальною мережею Інтернет. Разом з тим, доступність комп'ютерної техніки, мережі Інтернет та «хмарних» технологій надають змогу обізнаному в інформаційних технологіях зловмиснику застосовувати свої знання для вчинення кіберзлочину з будь-якої точки планети, у будь-якому населеному пункті, провівши атаку на об'єкти, які можуть знаходитись за тисячі кілометрів від нього.

Розслідування такого роду злочинів не є цілковитою новинкою для вітчизняних правоохоронних органів. Разом з тим, на думку О. А. Парфило, Ю. Ю. Нізовцева, все ще залишається доволі складно виявляти, фіксувати і вилучати криміналістично значиму інформацію при розслідуванні вказаної категорії злочинів для використання її надалі в якості доказової інформації. Причинами цього є і нестача кваліфікованих кадрів, на достатньому рівні обізнаних в інформаційних технологіях, і відсутність належної кількості спеціального криміналістичного обладнання, а також брак практики розслідування таких злочинів тощо [1, с. 148].

Саме тому, актуальним є питання організації і проведення слідчих (розшукових) дій під час розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж, що має певні особливості та вимагає від слідчого як особистого володіння спеціальними знаннями та навичками, так і використання допомоги осіб, що на високому рівні володіють такими знаннями [2, с. 113].

Відповідно до кримінального процесуального законодавства України спеціальні знання можуть використовуватись у двох формах: при залученні спеціалістів для надання безпосередньої технічної допомоги під час досудового розслідування чи консультацій з питань, що потребують відповідних спеціальних знань, та в межах проведення відповідної експертизи.

Незважаючи на певний рівень володіння потрібними знаннями у цій галузі, під час підготовки до проведення слідчих (розшукових) дій слідчому необхідно вирішити питання щодо залучення до цього певного кола спеціалістів. Так, на думку Є. Д. Лук'янчикова, залучення осіб, що володіють спеціальними знаннями до проведення слідчих дій обумовлюється необхідністю використання сучасних досягнень у сфері комп'ютерних систем та інформаційних технологій.

Використання допомоги зазначених осіб дозволить своєчасно визначати індивідуальний почерк роботи програміста й ідентифікаційних характеристик розроблених ним програм, перелік електронних адрес і сайтів Інтернет, якими оперував користувач. Спеціаліст допоможе дослідити матеріальні носії з метою пошуку відповідної інформації та провести ідентифікацію комп'ютерних систем за слідами на різних матеріальних носіях інформації [2, с. 113–114].

Аналіз наукової літератури та матеріалів практики дозволяє виділити декілька варіантів залучення обізнаних осіб до участі в розслідуванні кіберзлочинів, серед яких:

1) співробітники експертних установ Міністерства юстиції або МВС України, які володіють знаннями, що необхідні для пошуку, фіксації, вилучення та дослідження комп'ютерних слідів злочину; мають документи, що підтверджують їх кваліфікацію; проходять періодичну професійну перепідготовку і підвищення кваліфікації; не мають особистого інтересу у конкретному провадженні;

2) спеціалісти з ІТ-технологій інших підприємств, організацій, установ, щодо яких Є. Д. Лук'янчиков пропонує створювати постійний список, періодично його переглядати та оновлювати, за відповідними критеріями. Зазначена організація цієї роботи сприятиме підвищенню професійного рівня зазначених осіб, забезпечить результативність їх допомоги слідчому. Періодичне їх залучення до участі у слідчих діях сприятиме формуванню у них цілеспрямованих пошукових навичок. Такий спеціаліст може виявити спеціальні засоби, встановлені власником в комп'ютері для знищення інформації при несанкціонованому доступі; встановити необхідний пароль для доступу до інформації, з'ясувати правила його використання і чи не призведе порушення цих правил до знищення файлів тощо [2, с. 114].

Слід також зазначити, що вчинення кіберзлочинів супроводжується виникненням специфічних слідів, які в криміналістичній літературі називають «віртуальними», «цифровими» або «електронними» Це, на думку О. І. Тригубчак, обумовлене тим, що вказані сліди є нетрадиційними, візуально не сприймаються, а виявляються в результаті проведення експертних досліджень. Експертиза, за допомогою якої встановлюються сліди кіберзлочинів іменується в літературі комп'ютерно-технічною [3, с. 204]. Згідно з Інструкцією Міністерства юстиції України про призначення та проведення судових експертиз відповідні дослідження здійснюються в межах експертизи комп'ютерної техніки і програмних продуктів та експертизи телекомунікаційних систем та засобів [4].

Об'єктами такого виду дослідження є носії комп'ютерної інформації, мережі і їх складові частини, мобільні термінали тощо. Крім того, з метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки. Слід також погодитись з думкою О. І. Тригубчак, яка зазначає, що розвиток комп'ютерної техніки призведе до появи нових носіїв інформації і відповідно до нових видів комп'ютерно-технічної експертизи [3, с. 205].

Отже, можна зробити висновок, що використання спеціальних знань шляхом залучення спеціаліста чи експерта значно підвищить результативність та полегшить роботу слідчого під час розслідування кіберзлочинів.

Список бібліографічних посилань: 1. Парфило О. А., Нізовцев Ю. Ю. Щодо проблем збирання доказів при розслідуванні кіберзлочинів // Досудове розслідування: актуальні проблеми та шляхи їх вирішення: матеріали наук.-практ. семінару (Харків, 17 жовт. 2014 р.). Харків: Право, 2014. Вип. 6. С. 147–151. 2. Лук'янчиков Є. Д., Лук'янчиков Б. Є. Участь спеціаліста при розслідуванні комп'ютерних злочинів // Актуальні питання розслідування кіберзлочинів: матеріали Міжнар. наук.-практ. конф. (м. Харків, 10 груд. 2013 р.) / МВС України; Харків. нац. ун-т внутр. справ. Харків, 2013. С. 113–115. 3. Тригубчак О. І. Структура та зміст типової методики комп'ютерно-технічної експертизи // Актуальні питання розслідування кіберзлочинів: матеріали Міжнар. наук.-практ. конф. (м. Харків, 10 груд. 2013 р.) / МВС України; Харків. нац. ун-т внутр. справ. Харків, 2013. С. 204–207. 4. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 8 жовт. 1998 р. № 53/5 // База даних «Законодавство України» / Верховна Рада України. URL: <http://zakon.rada.gov.ua/laws/show/z0705-98> (дата звернення: 03.10.2017).

Одержано 08.10.2017

УДК 343.98

Володимир Васильович ЛИСЕНКО,

професор кафедри кримінального процесу та криміналістики
Університету державної фіскальної служби України,
доктор юридичних наук, професор;

Олена Володимирівна ЛИСЕНКО,

кандидат юридичних наук, керівник
комунікативного напрямку ГО «Юридична сотня»

НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ДІЇ В РОЗШУКОВІЙ РОБОТІ СЛІДЧОГО

Прийняття нового кримінального процесуального законодавства відкрило шлях для широкого застосування можливостей оперативно-розшукової діяльності у розшуковій роботі слідчого. Це дозволило розширити інструментарій у ході досудового розслідування, а також можливості слідчого у здійсненні розшуку осіб, які переходять від досудового розслідування. На сьогодні складно уявити діяльність правоохоронних органів із встановлення місцезнаходження осіб, які переходять від досудового розслідування, без використання спеціальних заходів. До таких заходів, зокрема, можуть бути віднесені негласні слідчі (розшукові) дії та комплекс відповідних оперативно-розшукових заходів. Проведення зазначених вище дій має свою специфіку щодо організації та проведення у ході досудового розслідування, в тому числі для організації розшуку осіб.

Про можливість та необхідність застосування негласних слідчих (розшукових) дій у розшуковій роботі слідчого визначено, зокрема, у ч. 2 ст. 246 КПК України, де зазначається, що негласні слідчі (розшукові) дії проводяться у випадках, якщо відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб. У ст. 267 КПК України, яка визначає особливості проведення такої негласної слідчої дії як обстеження публічно недоступних місць, житла чи іншого володіння, прямо зазначається про мету проведення