Мислива Оксана Олегівна
старший викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ВИЯВЛЕННІ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ, ПОВ'ЯЗАНОЇ З ТРАНСПЛАНТАЦІЄЮ

Розвиток технологій трансплантації спричинив появу на початку XX століття нового виду суспільно небезпечної протиправної діяльності, яка стрімко набула поширення у зв'язку з можливістю отримувати від неї значні прибутки. А розвиток у XXI столітті інформаційних технологій інтегрував їх у кіберпростір. За допомогою нових технологій транснаціональна злочинність отримала нову форму існування та механізми здійснення незаконної діяльності.

Наявність значного числа мережних сховищ, соціальних мереж та інших мультимедійних засобів спілкування, безкоштовних VPN і TOR-мереж, фішингових і гібридних сайтів, запровадження криптовалюти та інших технологій «розв'язують руки» злочинцям, надаючи їм можливість майже безконтрольно та безпечно передавати інформацію в мережах для укладення незаконних угод стосовно людини та частин її тіла, вербувати або підшукувати донорів органів або тканин чи потенційних жертв шляхом комунікації в соціальних мережах або реклами в інтернет-мережах, шантажувати їх із забезпеченням власної анонімності, відмивати кошти, отримані від злочинної діяльності тощо. Використання технологій дозволяє здійснювати злочинну діяльність або пособництво в ній завдяки використанню таких звичних засобів, як смарт-телефонів, комп'ютерів, ноутбуків і планшетів, які широко поширені.

Міжнародна практика протидії торгівлі людьми, з якою безперечно пов'язана незаконна діяльність у сфері трансплантації, переконує, що досить важко виявити та розслідувати такі злочини, зокрема, задокументувати їх належним чином. Статистика свідчить, що в Україні кількість облікованих кримінальних правопорушень за ст. 149 КК України (торгівля людьми) суттєво зросла [1, с. 9]. Якщо протидія торгівлі людьми з метою їх експлуатації в порнобізнесі, особливо дітей, просувається більш-менш вдало завдяки новостворених підрозділам з протидії кіберзлочинності, інвестуванню в цю правоохоронну сферу іноземних інвестицій та значної уваги до цього питання міжнародної спільноти, то виявлення та розкриття злочинів, пов'язаних з трансплантацією, в силу їх більшої латентності традиційно ще більш ускладнені. Злочинів у сфері трансплантації реєструється значно менше, чим виявляється, а виявлені за недостатністю доказів закриваються, в тому числі, у суді. Крім іншого, це свідчить про низьку ефективність організації з їх виявлення та документування. Зокрема, ці злочини вчиняються традиційними методами, а використання інформаційних технологій дозволяє лише підготувати злочин, здійснювати пособництво в ньому. Вину безпосереднього організатора чи виконавця на стадії виявлення злочину важко довести.

Доцільність виявлення злочинної діяльності у сфері трансплантації прямо пропорційна реалізації доказів винуватості правопорушників під час розслідування. Якщо виявити злочин може особа, яка не володіє спеціальними знаннями за допомогою огляду веб-сайтів, аналізу даних соціальних мереж, оформлення запиту у провайдера щодо власника IP-адреси, то складність документування пов'язана з необхідністю залучення спеціаліста, який має достатній технічний рівень знань, досвід правильного застосування алгоритму вилучення доказів із мережевої системи, в тому числі, в режимі реального часу, криміналістичні інструменти і досвід роботи з ними для того, щоб ці докази були визнані належними у суді [1, с. 108].

Водночас, основною тенденцією у застосуванні інформаційних технологій під час злочинної діяльності є пошук та вербування жертв-донорів через соціальні мережі (самі подають оголошення) або на спеціально створених публічних веб-сайтах, наприклад, агенцій із працевлаштування, шлюбні агентства чи туризму, сайти знайомств, лікування за кордоном тощо. Подальше спілкування між злочинцем і жертвою може відбуватися через чати, інтернет-пейджери, захищені засоби (WhatsApp) та VoIP-технології. Останні з них мають надзвичайний ступінь шифрування, що заважає перехоплювати зміст і метадані (skype,

viber) без встановлення використання програми WireShark.

Виявлення незаконної діяльності у сфері трансплантації нині не може базуватись на традиційних тактичних прийомах і методах проведення подальших слідчих та негласних слідчих (розшукових) дій. Серед методів виявлення злочинців слід визначити спеціальне програмне забезпечення, розподілені обчислення та негласну роботу. Ідентифікацію злочинця дозволяє отримати як звернення до Інтерполу (WHOIS?), так і власний пошук інформації (встановити домен та хостинг), здійснити офіційний запит і отримати рішення суду на вилучення історії листування), зняття інформації з транспортних телекомунікаційних мереж відповідно до ст. 263 КПК України – контроль передачі СМС, ММС, факсом чи модемом стосовно даних про зустрічі, винагороду, характер угоди та інше.

Як свідчить досвід роботи Canadian Police Centre for Missing and Exploited Children/Behavioural Sciences Branch у протидії дитячим грумінгу та порнографії, велике значення для виявлення та розкриття злочинів є імітація зацікавленості у злочинній активності (наприклад, під приводом потреби лікування трансплантацією імітація покупця чи замовника біологічних матеріалів або торгівлі власними органами), використовуючи псевдонім, рейковий аккаунт та програмні безкоштовні засоби запису з монітору в режимі онлайн (EatCam Web Recorder) та збереження листування в соцмережі [2].

Підсумовуючи слід зазначити, що удосконалення системи підготовки правоохоронців і спеціалістів з ІТ-технологій, вироблення форм і методів їх щільної співпраці, проведення комплексу досліджень з виявлення та розслідування різних видів злочинів за допомогою інформаційних технологій, удосконалення законодавства у сфері проведення подальших слідчих та негласних слідчих (розшукових) дій, а також використання позитивного світового досвіду та розвиток партнерства стане запорукою ефективності забезпечення діяльності у протидії транснаціональній та кіберзлочинності.

1. Навчальний курс з виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. -148 с.
2. Cory Patterson. Internet Facilitated Crime, Child Exploitation, Past, Present and the Future Canadian: Ukraine Presentation #1 / Royal Canadian Mounted Police Saskatchewan Internet Child Exploitation Unit : Police Centre for Missing and Exploited Children/Behavioural Sciences Branch. - Canada, 2017. – 18 p.

Міщанинець Олександр Миколайович
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ
кандидат юридичних наук,

ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ ЯК ФУНКЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Державний механізм забезпечення правоохоронної діяльності та функціонування правоохоронних органів в нашій державі щодо протидії злочинності передбачає різноманітні форми його здійснення: соціальні, економічні, культурно-виховні, кримінально-правові та інші. Серед державно-правових форм протидії злочинності особливе місце належить оперативно-розшуковій діяльності.

Оперативно-розшукова діяльність як одна із функцій правоохоронних органів здійснюється з метою виявлення, запобігання та припинення злочинів, отримання інформації в інтересах кримінального судочинства, а також безпеки суспільства і держави.

Саме протидії злочинам є основою для усіх теорій як кримінального права, кримінального процесу, кримінально-виконавчого права, кримінології, криміналістики, так і оперативно-розшуковій діяльності.

Слід погодитись із думкою В.С. Зеленецького, що теорія оперативно-розшукової діяльності розроблює лише особливий аспект діяльності відповідних органів і тому не може включати в свій предмет загальні питання протидії злочинності.

Узагальнення практичного досвіду оперативно-розшукової протидії злочинам та аналіз