льне і приховане спостереження за об'єктом злочину; гарне технічне оснащення та озброєність членів ОГ та ЗО.

Оперативно-розшукова тактика розробляє прийоми і рекомендації здійснення тактичних оперативних заходів і операцій, як затримання або знешкодження озброєних злочинців, ліквідації бандитських угруповань, реалізації комплексних оперативно-розшукових заходів та НС(Р)Д. Моделювання, як елемент тактики, виконуючи пізнавальну роль, дозволяє визначити коло осіб, причетних до вчинення злочину членами ОГ та ЗО. Зокрема, уявна модель кримінальної події формується у свідомості оперативного працівника на основі отриманої інформації. Прогнозування використовується для вироблення правильної програми дій і прийняття управлінських рішень, що забезпечують досягнення найкращих результатів при виконанні завдань протидії організованій злочинності.

Література:

1. Недопущення типових помилок документування діяльності організованих злочинних груп: метод. рек. МНД УП БОЗ при РНБО України, ГПУ, НАПУ; авт.: М.В. Гребенюк, І.І. Тупеляк, О.Б. Комарницька та ін. Київ. 2018. 84 с.

2. Бандурка О.М. Стратегія і тактика протидії злочинності: монографія. О.М. Бандурка, О.М. Литвинов. Харків. 2012. 318 с.

3. Особливості кваліфікації та розслідування злочинів, учинених організованими групами та злочинними організаціями. метод. рекоменд. Вознюк А.А., Чернявський С.С., Татаров О.Ю., Цюприк І.В., Чернєй В.В.; МВС України, Головне слідче управління, НАВС. 2013. 55 с.

4. Оперативно-розшукова діяльність. навч. посіб. Є. М. Моісеєв, О. М. Джужа, Д. Й. Никифорчук та ін. за ред. проф. О. М. Джужи. К. 2009. 310 с.

О.А. Самойленко,
к. ю. н., доцент, доцент кафедри криміналістики
Національного університету «Одеська юридична академія»

ПИТАННЯ ПЕРСОНАЛІЗАЦІЇ ВІДОМОСТЕЙ ПРО ОСОБУ ЗЛОЧИНЦЯ, ЩО ВЧИНЯЄ КРИМІНАЛЬНЕ ПРАВОПОРУШЕННЯ У ОБСТАНОВЦІ КІБЕРПРОСТОРУ

У більшості праць з тематики типізації слідчих ситуацій розслідування кіберзлочинів науковці залишають поза увагою відомості про особу злочинця. Криміналісти акцентувались на несанкціонованому доступі до предмета посягання, оскільки потерпілій стороні простіше заявити про несанкціонований доступ, ніж визнати свою неспроможність забезпечити максимально захищений санкціонований доступ, обрати висо-

кокваліфікований, без кримінальних схильностей персонал мережі. В цьому контексті дослідник М. В. Богомолов зазначає, що спеціалізовані інформаційні системи дедалі частіше намагаються ізолювати у мережі Інтернет, тому приховати вчинення злочину внутрішнім користувачем стало значно складніше [1, с. 15]. За таких умов під час висвітлення питань типізації слідчих ситуацій початкового етапу розслідування вказаної категорії злочинів факт або можливість персоналізації відомостей про користувача-злочинця сьогодні не можна ігнорувати. Розширення спектру злочинів, вчинених у кіберпросторі, також зумовило потребу продовження наукового пошуку оптимального підходу до типізації слідчих ситуацій розслідування злочинів, вчинених у кіберпросторі, та визначення в цьому контексті значення відомостей про особу(групу осіб), яка вчинила злочин, на момент відкриття кримінального провадження.

Персоналізувати особу конкретного користувача як злочинця-користувача дозволяє визначеність у матеріалах, що передані слідчому в рамках процедури відкриття кримінального провадження, відомостей про користувача веб-сторінки соціальної мережі, дошці оголошень чи іншій технології, що використовується у механізмі вчинення злочину, дані абонентського номеру користувача, його IP-адреси, MAC-адреси обладнання, що використовувалась при вчиненні або готуванні злочину в кіберпросторі.

Слід підкреслити, що безпосередній власник інформації в системі визначає перелік користувачів (фізичну або юридичну особу) та їх повноваження стосовно цієї інформації. Остання фізично розміщена в комп'ютерному обладненні, об'єднаному каналами зв'язку з цією мережею, яке в мережі має свій ідентифікатор – IP-адресу [2, с. 39-40] та MAC-адресу. Основними відомостями про власників інформації та її користувачів є IP-адреси та MAC-адрес. Отримання цієї інформації ідентифікує обладнання та точку доступу конкретного користувача, але по-суті це не персоналізовані відомості конкретного користувача, адже персональні дані особи, яка знаходиться у точці доступу за конкретним комп'ютерним устаткуванням та вчиняє злочин, не завжди є постійним користувачем у мережі. Для розуміння цього потрібно звернутись до основ слідоутворення у кіберпросторі.

IP-адреси – це унікальна адреса (ідентифікатор) вузла в мережі, яка збудована на проколах IPv4, IPv6, що для зручності сприйняття має вигляд десятково-крапковій нотації. IPv4-адрес складається з чотирьох груп цифр (октетів) у діапазоні від 0 до 255, розділених крапками (наприклад, ip-addr: 195.47.253.2). IPv6-адреса складається з восьми блоків, кожен з яких включає по чотири шістнадцяткові цифри; блоки розділені двокрапкою (наприклад ipv6-addr: 2001:67c:258:2). Унікальність IP-адрес забезпечується централізованим розподілом діапазонів адрес

Адміністрацією адресного простору Інтернет (Internet Assigned Numbers Authority – IANA) між регіональними інтернет-реєстраторам (Regional Internet Registries – RIR), які розподіляють IP-адреси серед провайдерів. Значення IP-адреси в контексті механізму слідоутворення детально описано в дисертації С. В. Самойлова [3]. В результаті аналізу спеціалізованої літератури автор визначив важливі для розуміння процесу слідоутворення власивості IP-адрес, а саме:

1)через те, що протокол IP є основним протоколом у мережі «Інтернет» - всі вузли в цій мережі для коректної адресації мають власні унікальні IP-адреси;

2)в мережі «Інтернет» двом різним вузлам в один проміжок часу не може бути присвоєна одна IP-адреса;

3)як IP-адресу вузла в мережі «Інтернет» можуть бути призначені лише адреси з певного діапазону;

Кожний процес передачі даних у мережі «Інтернет» супроводжується багаторазовою передачею IP-адреси, що обумовлено фрагментацією даних та неодноразовістю сеансів підключення до ресурсу. Іншими словами, при кожному підключенні до сервісу, відвідуванні сайту, відправленні електронного листа чи просто підключенні до мережі «Інтернет» залишаються записи IP-адреси [3, с. 76-77]. С. В. Самойлов справедливо висновує про те, що через реалізацію зазначених функцій має місце процес слідоутворення, отже IP-адреса, з якої виконувалось підключення до мережі «Інтернет» та проводились операції взаємодії з ресурсами цієї мережі, є не чим іншим, як слідом. При цьому фактично IP-адреса є лише умовою, яка дозволяє в подальшому шляхом здійснення слідчих (розшукових) дій встановити як користувача, так й володільця інформацією.

MAC-адреси (Media Access Control address, MAC-address або адреса управління доступом до середовища) – це унікальне 48-бітне число, запрограмована виробником під час виробництва конкретного екземпляру комп'ютерної техніки, що складається з шести частин із чисел у шістнадцятковому вигляді, наприклад 01:B7:A3:OB:E1:19. Щоразу, коли пристрій зв'язується з мережею Інтернет, DHCP-сервер надає його MAC-адресі вільну IP-адресу зі списку наявних динамічних адрес. Криміналістична значущість MAC-адреси як сліду від використання пристрою в мережі полягає в тому, що вона прямо вказує на пристрій (мережеву плату, принтер, маршрутизатор, сервер тощо) тобто є його ідентифікатором. Наявність MAC-адресу теж лише дозволяє в подальшому встановити персональні дані злочинця-користувача.

Варто підкреслити, що поява та інтенсивний розвиток технологій анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій, або англ. Virtual Private Network) інших засобів-анонімайзерів) має наслідком

учинення злочинів якісно нового рівня організації злочинної діяльності. Використання технологій анонімайзерів дозволяє забезпечувати конфіденційність інформації про користувача з метою отримання останнім доступу до заборонених у локальній мережі веб-сайтів, доступ до яких громадянам певної країни заблокований рішенням державних органів цієї країни. Наприклад, користувач заходить на веб-сайт, що надає послугу анонімайзера, вводить в адресний рядок адресу веб-сторінки, яку користувач бажає відвідати анонімно. Анонімайзер завантажує цю сторінку собі, обробляє її та передає користувачу, але вже від свого (сервера-анонімайзера) імені. В іншому разі технологія TOR (браузер) аналогічно дозволяє отримати анонімний доступ до певних ресурсів Інтернет шляхом так званої «цибулевої маршрутизації». Для передавання інформації використовуються три довільні Інтернет-вузли. Tor-браузер (Tor Browser) відправляє першому вузлу пакет із зашифрованою адресою другого вузла. Перший вузол має ключ для розшифрування адреси та переправляє інформацію на другий вузол. Останній, одержавши пакет, має ключ для розшифрування адреси третього вузла. Таким чином, для правоохоронних органів стає незрозумілим, який саме сайт особа запитувала та відвідала в результаті через вікно Tor-браузера. Ці та аналогічні програмні засоби з мережі Інтернет вільно завантажує будь-який користувач. Використання таких технологій створює безмежні можливості для вчинення злочинів різної тяжкості: від створення ринків збуту товарів, заборонених до цивільного обігу (наркотиків, зброї), поширення порнографії, порушення авторських прав до терористичних актів.

Таким чином, в момент відкриття кримінального провадження ступінь повноти вихідної інформації про злочин буде визначається перш за все характером інформації про особу злочинця, зокрема може бути описаний як :

1)наявність персоналізованих відомостей (розгорнуті анкетні дані особи злочинця);

2) наявність неперсоналізованих відомостей (IP-адреси, MAC-адреси, сторінка у соціальній мережі тощо);

3) відсутність персоналізованих та неперсоналізованих відомостей (через використання злочинцем технологій анонімізації доступу до ресурсів Інтернет, індивідуальної географічної мобільності). Ці групи інформації про особу злочинця можуть бути використані з метою подальшої типізації слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі.

Література:

1. Богомолов М. В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации: дис. …

канд. юрид. наук: 12.00.08. Красноярск, 2002. URL: https://legalns.com/download/books/lib/criminalistics/book-001.pdf

2. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін.; за заг. ред. М.В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

3. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. 226 с.

Г.М. Симонова,
студентка магістратури факультету №2 ННІЗДН
Одеського державного університету внутрішніх справ
А. О. Шелехов,
к. ю. н., доцент, завідувач кафедри
публічного управління та адміністрування
Одеського державного університету внутрішніх справ

ОКРЕМІ ПИТАННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Останнім часом проблема транснаціональної злочинності виходить на новий рівень. Більшість світових експертів на основі аналізу активності транснаціональних організованих злочинних угрупувань дотримуються думки, що діяльність таких угрупувань стала головною загрозою XXI сторіччя.

Загроза діяльності організованих злочинних угрупувань на сьогоднішній день набагато серйозніша за терористичну, яка не володіє необхідними силами та засобами для того, щоб підривати основи безпеки тієї чи іншої держави. Відповідно до ст. 1 Закону України «Про боротьбу з тероризмом» тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [1]. У той же час організована злочинна група згідно ст. 2 Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності визначається як структурно оформлена група в складі трьох або більше осіб, що існує протягом визначеного періоду часу і діє узгоджено з метою здійснення одного або декількох серйозних злочинів або злочинів, визнаних такими відповідно до Конвенції, для того, щоб одержати, прямо або посередньо, фінансову або іншу матеріальну вигоду [2]. Так, на відміну від терористичних груп, які намагаються зая-