О.С. СТУПАКОВ,
студент IV курсу
(Академія адвокатури України)
(Науковий керівник кандидат юридичних наук
В.І. Бояров)

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ОПЕРАТОРІВ МОБІЛЬНОГО ЗВ'ЯЗКУ, ВИРОБНИКІВ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ ПІД ЧАС РОЗКРИТТЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Ключові слова: *абонент, виробник мобільних операційних систем, відомості, мобільний телефон, оператор мобільного зв'язку.*

Сучасна криміналістика відіграє провідну роль у процесі розкриття та розслідування кримінальних правопорушень. Особливе місце в системі криміналістики належить криміналістичній техніці. Криміналістичні засоби і методи широко застосовуються в ході негласних слідчих (розшукових) дій, а також в процесі криміналістичних експертиз [7, 70].

Визначена законодавцем система науково-технічних засобів, що застосовуються для ефективної реалізації завдань кримінального судочинства, не є незмінною константою. З часом суб'єкти криміналістичної діяльності, з цілком логічних причин ходу суспільного буття, запроваджують до процесу розкриття та розслідування кримінальних правопорушень нові науково-технічні засоби [6, 28].

Останнім часом важливим джерелом отримання інформації про осіб, які вчинили кримінальне правопорушення, а також причетних до його вчинення, для працівників внутрішніх справ стають відомості, що надаються операторами мобільного зв'язку.

Загальновідомо, що компанії-провайдери мобільного зв'язку використовують ідентифікуючі службові сигнали для визначення місцезнаходження абонента в конкретний проміжок часу. Точність даних визначень залежить від цілого ряду факторів: топографії місцевості, наявності перешкод, кількості працюючих телефонів у даній «соті».

За допомогою ідентифікуючих службових сигналів компанії-провайдери мобільного зв'язку можуть надати працівникам органів внутрішніх справ важливу інформацію.

Відомості щодо наданих телекомунікаційних послуг (у тому числі факт отримання послуг, їхня тривалість, зміст, маршрути передавання тощо): а) за відомим номером абонента можливе встановлення IMEI (International Mobile Equipment Identifier – це п'ятнадцятизначне число, яке є унікальним для кожного мобільного

телефону, встановлюється заводом-виробником при виготовленні апарату для точної та повної ідентифікації телефону в мережах GSM та UMTS) коду терміналу або IMEI кодів всіх терміналів, якими користувався даний абоненту зазначений період часу; б) за відомим IMEI кодом терміналу можливе встановлення номера абонента або всіх номерів абонентів, які користувалися даним терміналом у зазначений період часу; в) вибірка вхідних/вихідних дзвінків конкретного абонента у зазначений період часу; г) встановлення місця перебування (в межах соти) конкретного терміналу і прив'язкою до часу; ґ) встановлення номерів ваучерів поповнення балансу абонента, з метою встановлення місця придбання; д) відслідкування переміщення коштів з балансу одного абонента на баланс іншого; е) вибірка всіх активних терміналів, які знаходилися в певному квадраті місцевості у певний час; є) встановлення номера абонента користувача Інтернету за допомогою мобільного терміналу за протоколом, у разі якщо відома його IP адреса і час виходу в Інтернет під нею; ж) постановка на облік певного номера абонента або IMEI номера терміналу з подальшим повідомленням замовника в разі появи вказаних абонентів або терміналів в мережі; з) за допомогою додаткових програмно-апаратних комплексів, встановлених на площадці оператору можлива постановка на відслідкування зразка голосу конкретної особи із встановленням IMEI номера терміналу, номера абонента; и) у разі, якщо дана особа починає сеанс голосового зв'язку, відповідно можливо вести запис розмов даної особи, незалежно яким терміналом або абонентським номером вона користується (кожна особа має притаманний їй тембр, висоту, емоційне забарвлення голосу) [1, 107].

Відомості про споживача, отримані при укладанні договору: а) прізвище, ім'я, по батькові; б) місце реєстрації, фактичного проживання; місце роботи, посада; в) реєстраційні дані документа, яким підтверджуються особисті дані (паспорт, посвідчення водія, службове посвідчення працівника органів державної влади або місцевого самоврядування) – серія, номер, коли, ким і де виданий; г) ідентифікаційний код; ґ) назва, код ЄДРПОУ, банківський рахунок, назва банку та МФО, номер свідоцтва платника ПДВ, код платника ПДВ, юридична адреса, прізвище, ініціали уповноваженої особи, адреса доставки кореспонденції, контактний телефон, адреса електронної пошти для абонента-юридичної особи тощо.

Безумовно важливим є те, що відомості, отримані від операторів мобільного зв'язку, можуть бути використанні для встановлення: факту вчинення кримінального правопорушення; часу, місця, способу вчинення кримінального правопорушення; осіб, що скоїли кримінальне правопорушення (у тому числі співучасників та причетних осіб); місцезнаходження викраденого майна тощо.

Принагідно зауважимо, що виробники мобільних операційних систем (Apple, Google та ін.) також відіграють важливу роль у процесі отримання інформації під час розкриття і розслідування кримінальних правопорушень.

Процес отримання інформації від виробників мобільних операційних систем, ми розглянемо на конкретних прикладах. Зокрема, коли особа активує свій мобільний телефон, планшет, вона вводить свої реєстраційні дані в програми, які розроблені виробниками мобільних операційних систем для подальшого повноцінного використання всіх функцій цих пристроїв. Це такі дані як: країна проживання, прізвище, ім'я, електронна адреса, номери кредитних карток. Такими Програмами можуть бути Itunes, Zyne, профіль Google і тд. Наприклад, без реєстраціє неможлива купівля навігаційних систем, електронних книжок, ігор в інтернет-магазинах (Play Market, App Store і тд.).

Іншим прикладом може бути використання системи GPS (Global Positioning

System – це супутникова навігаційна система, яка дозволяє визначати координати, швидкість і напрямок руху об'єктів в будь-якій точці земної кулі, в будь-який час доби, за будь-якої погоди) на нашому мобільному телефоні. Коли ми вмикаємо функцію визначення місцезнаходження, операційна система пропонує прийняти умови використання. У такий спосіб, компанія-виробник мобільних операційних систем попереджує, що вона має право збирати інформацію про місцезнаходження та переміщення особи. Дана інформація зберігається на серверах компанії-виробника мобільних операційних систем і в подальшому використовується для розроблення графіків популярності мобільних телефонів, поліпшення якості обслуговування споживачів тощо. В свою чергу, для криміналістики, така інформація також може бути корисною в процесі розкриття та розслідування кримінальних правопорушень. Вищезазначені компанії в основному співпрацюють на міжнародному рівні, але є і непоодинокі випадки сприяння розкриттю кримінальних правопорушень на місцевому рівні.

Необхідно зазначити, що законодавець регламентував процедуру проведення негласних слідчих (розшукових) дій у Главі 21 Кримінального процесуального кодексу України. Втручання у приватне спілкування (зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем) може проводитися за наявності чітко встановлених підстав: 1) відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб; 2) особа вчинила тяжкий або особливо тяжкий злочин. Дозвіл на втручання у приватне спілкування надає виключно слідчий суддя за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором [4].

Відповідно до Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, негласні слідчі (розшукові) дії, пов'язані зі зняттям інформації з транспортних телекомунікаційних мереж поділяються на: 1) контроль за телефонними розмовами (негласне проведення спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів із застосуванням відповідних технічних засобів); 2) зняття інформації з каналів зв'язку (негласне отримання, перетворення і фіксація різних видів сигналів, які передаються через лінії зв'язку мережі Інтернет, інших мережах передачі даних із застосування технічних засобів) [2].

Між тим, лунають пропозиції створення єдиної електронної системи, яка буде містити інформацію про абонентів для досягнення ефективних результатів розслідування та розкриття кримінальних правопорушень [5].

Разом з цим, ми хотіли би підкреслити, що відомості можуть бути отримані від операторів мобільного зв'язку, виробників мобільних операційних систем тільки у межах кримінального провадження. Якщо вони не можуть бути залучені до кримінального провадження, тоді їх слід використати для висунення версій, планування негласних слідчих (розшукових) дій та інших дій. При цьому, вся отримана інформація має ретельно перевірятися [1, 109].

Таким чином, виходячи з наведеного, зазначимо, що відомості, які можуть бути отримані від операторів мобільного зв'язку, виробників мобільних операційних систем відіграють вагому роль під час розкриття і розслідування кримінальних правопорушень, сприяють оперативному та ефективному вирішенню завдань кримінального провадження.

Список літератури:

1. *Вознюк А.А.* Використання ОВС можливостей операторів мобільного зв'язку під час розкриття та розслідування злочинів / А.А. Вознюк А.А., Д.О. Алексєєва-Процюк // Криміналістика XXI століття : матер. міжнар. наук.-практ. конф., 25-26 листоп. 2010 р. – Харків : Право, 2010. – 832 с.

2. *Інструкція про* організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Затверджено спільним наказом ГПУ, МВС, СБУ, АДПСУ, МФУ, МЮУ від 19 листопада 2012 р. № 114/1042/516/1199/936/1687/5 [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/GP12042.html

3. *Криміналістика. Академічний* курс : підручник / Т.В. Варфоломеєва, В.Г. Гончаренко, В.І. Бояров [та ін.]. — К. : Юрінком Інтер, 2011. – 504 с.

4. *Кримінальний процесуальний* кодекс України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/4651-17

5. *Синєокий О.В.* Інформаційне право України та електронне право високих технологій (електронний курс лекцій українською мовою) [Електронний ресурс] // О.В. Синєокий // Запоріжжя : ЗНУ, 2010. – 215 ел. с. – Режим доступу: http://nbuv.gov.ua/books/2010/10sovipu.pdf

6. *Скригонюк М.І.* Криміналістика : підручник // М.І. Скригонюк. – К. : Атіка, 2005. – 496 с.

7. *Шеремет А.П.* Криміналістика : навч. пос. [для студ. вищ. навч. закл.] / А.П. Шеремет. – [2-ге вид.]. – К. : Центр учбової літератури, 2009. – 472 с.

РЕЗЮМЕ

В статье проанализированы вопросы, связанные с работой операторов мобильной связи в контексте предоставления сведений об уголовном правонарушении правоохранительными органами. Отмечена актуальность использования возможностей разработчиков мобильных операционных систем и новых технических средств при раскрытии и расследовании уголовных правонарушений.

SUMMARY

The article represents the issues related with principles of mobile operators in the context of the provision information about the criminal offense to enforcement bodies. The author analyses the opportunities developers of mobile operating systems, and new techniques in the detection and investigation of criminal offense.

Рекомендовано кафедрою
кримінального процесу та криміналістики

Подано 10.10.2013.