МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ЛУГАНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ імені Е.О. ДІДОРЕНКА

**Бараненко Б.І., Бочковий О.В.,
Комарницький В.М., Кривонос М.В.**

ДІЯЛЬНІСТЬ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Науково-практичні рекомендації

Сєвєродонецьк
РВВ ЛДУВС ім. Е.О. Дідоренка
2019

УДК 351.741:343.85:004 (477) (072)
Д50

Авторський колектив:

Бараненко Б.І. – кандидат юридичних наук, професор;

Бочковий О.В. – провідний фахівець науково-дослідної лабораторії з проблем попередження, припинення та розслідування злочинів територіальними органами Національної поліції України Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, майор поліції, кандидат юридичних наук, старший науковий співробітник;

Комарницький В.М. – ректор Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, доктор юридичних наук, професор;

Кривонос М.В. – старший науковий співробітник науково-дослідної лабораторії з проблем попередження, припинення та розслідування злочинів територіальними органами Національної поліції України Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, майор поліції, кандидат юридичних наук

Рецензенти:

Колесник С.П. – начальник Головного управління Національної поліції в Луганській області, полковник поліції;

Шендрик В.В. – начальник кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ, полковник поліції, доктор юридичних наук, професор, заслужений юрист України.

Рекомендовано до друку та розповсюдження в мережі Інтернет Вченою радою Луганського державного університету внутрішніх справ імені Е.О. Дідоренка від 30 листопада 2018 року (протокол № 6)

Д50 Діяльності оперативних підрозділів Національної поліції України щодо протидії злочинам, які вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій: наук. практ. рекомендації / Б.І. Бараненко, О.В. Бочковий, В.М. Комарницький, М.В. Кривонос. Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е. О. Дідоренка, 2019. 110 с.

ISBN 978-617-616-084-7

У науково-практичних рекомендаціях висвітлено алгоритми дій працівників Національної поліції України під час організації виявлення, попередження, припинення й розслідування злочинів, що вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій.

Науково-практичні рекомендації призначені для працівників Національної поліції України, наукових та науково-педагогічних працівників закладів освіти зі специфічними умовами навчання, здобувачів вищої освіти.

УДК 351.741:343.85:004 (477) (072)

ISBN 978-617-616-084-7

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....4
ПЕРЕДМОВА.....5
Розділ 1. Поняття, основні види та особливості надання послуг і сервісів операторами та провайдерами телекомунікацій, які використовуються (застосовуються) або потенційно можуть бути використані під час вчинення злочинів.....7
Розділ 2. Особливості вчинення злочинів із застосуванням інформаційно-телекомунікаційних технологій на прикладі незаконного збуту наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів безконтактним способом.....28
Розділ 3. Процесуальний порядок фіксації протиправної інформації, розміщеної в мережі Інтернет.....45
Розділ 4. Зміст та правовий режим інформації про абонента та надані телекомунікаційні послуги, яка знаходиться в операторів та провайдерів телекомунікацій.....49
Розділ 5. Звернення до провайдерів телекомунікацій щодо надання інформації про користувачів мережі Інтернет і власників поштових скриньок.....56
Розділ 6. Тимчасовий доступ до інформації про абонента та надані телекомунікаційні послуги, яка знаходиться в операторів та провайдерів телекомунікацій.....62
Розділ 7. Отримання доступу працівниками карного розшуку до інформації, яка становить банківську таємницю.....72
Розділ 8. Види та джерела цифрових доказів, типові способи їх приховування, програмне забезпечення для їх виявлення та дослідження.....76
Розділ 9. Можливості й перспективи аналізу даних про події, осіб та їх зв'язки у протидії злочинам.....88
ДОДАТКИ.....100
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....104

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВССУЦКС – Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ

ДКР НП України – Департамент карного розшуку Національної поліції України

ЄРДР – Єдиний реєстр досудових розслідувань

ЗУ – Закон України

ІТ – інформаційні технології

КПК України – Кримінальний процесуальний кодекс України

н.п.а. – нормативно-правові акти

НП України – Національної поліції України

НС(Р)Д – негласні слідчі (розшукові) дії

ст. – стаття

ПЕРЕДМОВА

Протягом останніх років форми та способи підготовки, вчинення та приховування багатьох категорій злочинів зазнають суттєвих змін. Протиправні дії стають все більш законспірованими, при цьому все частіше злочинці використовують сучасні інформаційно-телекомунікаційні технології та інші досягнення науки та техніки.

Проблема протидії злочинам, які вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій не є новою для діяльності правоохоронних органів України, однак мають місце певні складнощі у практичній діяльності оперативних підрозділів Національної поліції України (далі по тексту – НП України) за вказаним напрямом роботи. Цьому сприяють: збільшення кількості злочинів, що вчиняються безконтактним способом із використанням закладок (схованок) та інформаційно-телекомунікаційних технологій, зокрема, незаконного обігу зброї, боєприпасів та вибухових речовин, наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, шахрайств тощо; недосконалість чинного кримінального й кримінального процесуального законодавства, відомчих нормативно-правових актів в частині законодавчого забезпечення правоохоронних органів належними засобами для протидії використанню мережі Інтернет та інших сучасних технологій у протиправних цілях; неналежна взаємодія між структурними підрозділами НП України в частині встановлення причетних до злочину осіб; відсутність відповідних методик виявлення, розслідування та профілактики злочинів, що вчиняються із використанням інформаційно-телекомунікаційних технологій; недостатня кількість компетентних фахівців та високотехнологічного програмного забезпечення й пошукового обладнання; висока латентність таких злочинів.

Особливого поширення набуває використання злочинцями у протиправній діяльності мережі Інтернет, мобільного зв'язку та основних сервісів, які надають провайдери телекомунікацій під час вчинення злочинів. Правопорушники вже давно оцінили технічні можливості сучасних інформаційно-телекомунікаційних технологій, можливості у будь-який час і будь-якому місці виходити на зв'язок зі співучасниками або обраними жертвами, дистанційно вчиняти протиправні дії, при цьому зберігати умовну або повну анонімність.

За сукупності викладених обставин тематика проведеного дослідження «Діяльності оперативних підрозділів Національної поліції України щодо протидії злочинам, які вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій», безсумнівно є актуальною й своєчасною. Зокрема для підрозділів карного розшуку Національної поліції України, які знаходяться на «передовій» у протидії злочинам та першими реагують на правові, організаційні й тактичні недоліки за вказаним напрямом діяльності. Своєчасність та необхідність дослідження проблем протидії злочинам, які вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій вилилось у замовленні ДКР НП України на проведення відповідного наукового дослідження.

Підготовлені авторами науково-практичні рекомендації мають практичну спрямованість та можуть бути використана при організації виявлення, попередження, припинення й розслідування злочинів, що вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій, а також у освітньому процесі закладів освіти зі специфічними умовами навчання.

РОЗДІЛ 1
ПОНЯТТЯ, ОСНОВНІ ВИДИ ТА ОСОБЛИВОСТІ НАДАННЯ ПОСЛУГ І СЕРВІСІВ ОПЕРАТОРАМИ ТА ПРОВАЙДЕРАМИ ТЕЛЕКОМУНІКАЦІЙ, ЯКІ ВИКОРИСТОВУЮТЬСЯ (ЗАСТОСОВУЮТЬСЯ) АБО ПОТЕНЦІЙНО МОЖУТЬ БУТИ ВИКОРИСТАНІ ПІД ЧАС ВЧИНЕННЯ ЗЛОЧИНІВ

Більшість визначень і термінів, що мають відношення до функціонування сфери телекомунікацій та надання телекомунікаційних послуг закріплені у базових нормативно-правових актах, а саме Законі України від 18.11.2003 № 1280-IV «Про телекомунікації», який встановлює правову основу діяльності у сфері телекомунікацій та Законі України від 02.10.1992 № 2657-XII «Про інформацію», який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та інших н.п.а.

Опорним поняттям цього дослідження є «*інформація*», яка виступає основним об'єктом інформаційного суспільства, роль якої сьогодні важко переоцінити. Відображаючи реальну дійсність, вона інтегрується у всі напрями діяльності держави, суспільства, громадянина, стаючи постійним і необхідним атрибутом забезпечення і реалізації їх функцій. Від її якості та достовірності, оперативності одержання залежить прийняття численних управлінських, процесуальних та інших рішень.

Поняття «інформація» використовується в усіх галузях науки, і в правовій, зокрема. Воно набуло багатозначності й інтерпретується залежно від сфери вживання.

В перекладі з латинської мови «інформація» (information) – це роз'яснення, виклад[1]. Тобто йдеться про

[1] Див.: Юридична енциклопедія: В 6 т. / редкол.: Ю.С. Шемшученко (голова редкол.) та ін. Київ: «Укр. енцикл.», 1998 – С. 717.

відомості (або їх сукупність), про предмети, явища й процеси навколишнього світу. У нормативно-правових актах під *інформацією* розуміють будь-які відомості (та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді), подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб[2].

Для того, щоб окреслити інформацію у правовому контексті, доцільно виділити такі юридично значимі ознаки, які зумовлюють специфіку інформації як об'єкта правового регулювання. До таких ознак слід віднести наступні:

- нематеріальний характер («самостійність відносно носія», тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона зафіксована);
- суб'єктивний характер («інформація виникає в результаті діяльності суб'єкта, який наділений свідомістю», тобто вона є результатом інтелектуальної діяльності);
- необхідність об'єктивації для включення у правовий обіг;
- кількісна визначеність;
- неспоживчість, можливість багаторазового використання;
- зберігання інформації у суб'єкта, який її передає;
- здатність до відтворення, копіювання, збереження і накопичення.

Отже, інформація – це об'єкт багатофункціональний. Вона створюється й застосовується в усіх сферах діяльності і забезпечує виконання багатоманітних функцій і завдань, що постають перед найрізноманітнішими суб'єктами. Не є виключенням і сфера, пов'язана із вчиненням злочинів та протидії їм з боку правоохоронних органів.

[2] Див.: ст. 1 «Про інформацію»: Закон України від 2 жовтня 1992 р. № 2658–XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12.

Наступним базовим визначенням є «*технологія*» – під якою розуміють комплекс наукових та інженерних знань, реалізованих у прийомах праці, наборах матеріальних, технічних, енергетичних, трудових факторів виробництва, способах їх з'єднання для створення продукту або послуги, що відповідають певним вимогам. Тому технологія нерозривно пов'язана з машинізацією виробничого або невиробничого, насамперед, управлінського процесу. Управлінські технології ґрунтуються на застосуванні комп'ютерної і телекомунікаційної техніки.

Інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Інформаційні технології, IT (використовується також загальніший / вищий за ієрархією термін *інформаційно-комунікаційні технології* (*Information and Communication Technologies, ICT*) – сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів.

Телекомунікаційні технології – це сукупність телекомунікаційних засобів, що забезпечують функції передачі, зберігання та обробки інформації. Ключовий компонент в розумінні технологій даного роду – це інформаційні мережі, навколо яких будується телекомунікаційна інфраструктура. У цьому процесі основна роль відводиться комп'ютерним системам та лініям передачі інформації.

Технології телекомунікацій – це принципи організації сучасних аналогових і цифрових систем, мереж зв'язку, включаючи комп'ютерні та Інтернет-мережі. Сучасні телекомунікаційні технології засновані на використанні телекомунікаційних мереж.

Телекомунікаційні мережі – система, що складається з об'єктів, які здійснюють функції генерації, перетворення, збереження продукту, і мають назву пункти (вузли) мережі, та ліній передач (зв'язку, комунікацій, з'єднань), що здійснюють передачу. До останніх можна віднести: телефонні мережі; радіомережу; телевізійні мережі; комп'ютерні мережі (Ethernet, Internet).

Телекомунікаційні мережі найчастіше розподіляють за територіальною ознакою на глобальні, регіональні та локальні. Це стосується не лише комп'ютерних мереж передачі даних, а й супутникових мереж, мереж мобільного зв'язку, служб поштових відправлень, радіо, телебачення тощо. Забезпечення міжмережевої взаємодії дозволяє створити гнучкий ефективний інструментарій для оптимізації процесів пошуку, розповсюдження, зберігання та відтворення інформації[3].

Засоби телекомунікацій – це сукупність технічних пристроїв, алгоритмів і програмного забезпечення, що дозволяють передавати дані по каналах зв'язку.

Термін *«телекомунікація»* («*теле*» від грец. τήλε – вдаль, далеко) – це частина слів, котрі вказують на їх зв'язок з далекою відстанню[4]. Відповідно «*комунікація*» (від лат. communicatio < communico – роблю спільним, сполучаю, спілкуюсь) – 1) повідомлення, шлях спілкування або зв'язок одного місця з іншим; 2) повідомлення, передача інформації від однієї людини до іншої[5]. Отже, це є передача та приймання певної інформації на віддаль від однієї особи до іншої або обмін інформацією на відстані.

[3] Див.: Тверезовська Н.Т., Нєлєпова А.В. Інформаційні технології в агрономії: навч. посібник. Київ: Центр учбової літ-ри, 2013. С. 59.

[4] Див.: Новейший словарь иностранных слов и выражений. Мн.: Харвест, Москва: ООО «Издательство АСТ», 2001. С. 778.

[5] Див.: Там само. С. 418.

Телекомунікаційна послуга – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій.

На сьогоднішній день оператори телекомунікацій надають фізичним та юридичним особам такі основні послуги, що забезпечують передачу та приймання певної інформації, а саме: послуги фіксованого телефонного зв'язку, послуги рухомого (мобільного) зв'язку та послуги із доступу до Інтернет. Значне поширення використання всіх зазначених типів зв'язку зумовлює потребу розглянути питання їх організації детальніше.

Рухомий (мобільний) зв'язок (його також називають «стільниковим») – електрозв'язок із застосуванням радіо технологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції. Функціонування мобільного зв'язку забезпечує стільникова структура зон зв'язку. Територія обслуговування стільникової системи мобільного зв'язку розподілена на окремі прилеглі одна до одної зони (соти). Обмін радіосигналами у кожній з таких зон забезпечується базовою станцією, яка має свою персональну територіально визначену адресу. Кожна окрема станція, у свою чергу, підключена до звичайної дротової телефонної мережі і оснащена технічними засобами, що перетворюють високочастотний сигнал мобільного телефону у низькочастотний сигнал стаціонарного (дротового) телефону і – в зворотному напрямі, що забезпечує сполучення обох систем[6].

[6] Див.: Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: монография. Москва: Издательство «Юрлитинформ», 2010. 192 с.

У найбільш поширеному на території України стандарті мобільного зв'язку GSM присутній процес, який має назву «Periodic Location Update» (періодичне оновлення місця розташування) та запускається внаслідок будь-якої події: вхідного або вихідного дзвінка; прийому або передачі SMS; включення або виключення телефонного апарату; зміни локального коду зони LAC (Location Area Code) у соті; зміни оператора при роумінгу; примусової перереєстрації у мережі в період, кратний шести хвилинам.

Кожна базова станція з певним інтервалом часу генерує службовий сигнал, який передається у формі невидимого службового повідомлення. Прийнявши його, мобільний телефон автоматично додає до нього свої MIN- і ESN-номери і передає кодову комбінацію на базову станцію. Унаслідок цього відбувається ідентифікація конкретного мобільного телефону, номеру рахунку його власника і «прив'язка» мобільного терміналу до певної зони, у якій він знаходиться в конкретний проміжок часу. У випадку здійснення телефонного дзвінка, базова станція виділяє користувачу одну з вільних частот тієї зони, в якій він знаходиться, та вносить відповідні зміни в його рахунок, передаючи виклик за призначенням. Якщо мобільний користувач під час розмови переміщується з однієї зони (соти) зв'язку до іншої, базова станція зони автоматично переводить сигнал на вільну частоту нової зони з більшим рівнем сигналу. Так, у кожному осередку знаходиться базова приймально-передавальна станція, що обслуговує всі абонентські радіотелефонні апарати у межах свого осередку (соти). У разі переміщення абонента з одного осередку в інший здійснюється передача його обслуговування іншій базовій станції[7]. Усі базові станції системи

[7] Див.: Використання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, їх транспортних телекомунікаційних мережах, під час розслідування злочинів: метод. рекомендації / С.С. Чернявський, О.Ю. Татаров, Д.О. Алексєєва-Процюк та ін. Київ: Нац. акад. внутр. справ, 2013. С. 6-7.

замикаються на центр комутації, який виконує роль обробки потоків інформації, що поступає від базових станцій, і реалізує функцію взаємодії з іншими операторами зв'язку: стаціонарною телефонною мережею, мережею міжміського зв'язку, мережею передачі даних і мережами інших операторів зв'язку. Крім того, центр комутації реєструє, ідентифікує абонентів, забезпечує захист інформації, оновлює інформацію про місцезнаходження абонентів, організовує передачу, обслуговування, маршрути викликів при роумінгу та ін.

Зв'язок між абонентами рухового зв'язку здійснюється за допомогою *мобільних телефонів* (мобільних терміналів). У кожний мобільний телефон виробником закладено унікальний міжнародний ідентифікаційний номер кінцевого обладнання (IMEI-код, що є постійним та незмінним* навіть при заміні SIM-карти), призначений для точної і повної ідентифікації пристрою у мережі. *Не зважаючи на вимогу до фірм виробників щодо недопущення випуску мобільних телефонів з однаковими IMEI-кодами, такі факти мають місце в мобільних телефонах з китайськими наборами мікросхем, які у переважній більшості нелегально потрапляють в Україну, не сертифікуються та активно використовуються під час вчинення злочинів. Крім цього, окремі несумлінні громадяни, які мають відповідну технічну освіту й навички та неофіційно займаються встановленням (оновленням) мобільного програмного забезпечення, за винагороду змінюють (або обнулюють) встановлений у мобільний теле-*

* Виключенням з цього правила є ситуації, коли зміна IMEI-коду мобільного терміналу відбувається внаслідок переустановлення програмного забезпечення (мобільної операційної системи).

фон виробником IMEI-код або продають мобільні телефони з вже «нульовими» IMEI-кодами[♦]*, що створює додаткові проблеми під час відслідковування руху даного мобільного пристрою (у випадках, коли мобільний пристрій був предметом злочину або використовувався як засіб для зв'язку під час вчинення злочину).*

Ідентифікація кінцевого обладнання абонента в телекомунікаційній мережі також здійснюється за допомогою змінної ідентифікаційної смарт-картки (SIM, USIM або R-UIM-картки тощо), мікрочип якої містить міжнародний мобільний ідентифікаційний номер абонента (IMSI) і секретний ключ для автентифікації.

До основних сервісів мобільного зв'язку, які надають оператори телекомунікацій належать:

SMS (Short Message Service) – послуга, що дозволяє передавати короткі (до 160 знаків) текстові повідомлення іншим абонентам.

MMS (Multimedia Messaging Service) – послуга, що дозволяє обмінюватися мультимедійними повідомленнями, які містять текст, відео, аудіо, графіку і інші файли, загальним розміром до 1 Мб.

Переадресація – послуга, що надає можливість перемикати всі вхідні виклики на будь-який інший телефонний номер в Україні. Виклики, що надходять на мобільний телефон, можуть бути переадресовані на телефон міської мережі або на будь-який мобільний телефон. Встановлена переадресація вхідних дзвінків не перешкодить здійснювати з телефону вихідні дзвінки.

Голосова пошта – послуга, що дозволяє абонентові не пропустити жодного дзвінка. Принцип її роботи аналогі-

♦ На сайті https://www.olx.ua окремі несумлінні ділки виставляють оголошення такого змісту: «Продам нові телефони без імей. Захищені від прослуховування, і місце положення не визначається. Оптом дешевше. Доставка Новою поштою по Україні. URL: https://www.olx.ua/obyavlenie/prodam-imey-000000000-IDtHJoU.html

чний автовідповідачу. Голосова пошта працює в сполученні з переадресацією, тобто вхідний дзвінок перенаправляється на голосову пошту для запису повідомлення на поштову скриньку абонента. Прослухати повідомлення абонент може в будь-який та зручний для себе час.

Доступ до мобільного Інтернету – послуга, що дозволяє одержувати доступ до інформації, що розміщена в текстовому вигляді на сайтах в мережі Інтернет.

Конференц-зв'язок – послуга, що дозволяє вести розмову одночасно шести абонентам (у компанії МТС), а також приймати виклики і відповідати на них під час розмови з іншими абонентами.

Роумінг – послуга, що дозволяє залишатись на зв'язку, перебуваючи за межами України, та отримувати широкий перелік якісних телекомунікаційних послуг (голосових дзвінків та SMS-повідомлень, передачі даних та MMS-повідомлень, відеотелефонії).

Оператор рухомого (мобільного) зв'язку створює і використовує банк даних, що містить відомості, надані абонентом під час укладення договору про надання послуг рухомого (мобільного) зв'язку та забезпечує його конфіденційність.

Істотно менш популярним і поширеним, у порівнянні з мобільним зв'язком, є *фіксований зв'язок,* який представляє собою телекомунікації, що здійснюються за допомогою телефонної мережі, яка представляє собою сукупність технічних споруд і устаткування, що призначене для здійснення телефонного зв'язку і складається з телефонних вузлів зв'язку, телефонних станцій, ліній зв'язку та кінцевих абонентських стаціонарних (нерухомих) терміналів (телефонних апаратів, оснащених номеронабирачем або клавіатурою для ручного введення телефонного номера). Телефонні апарати використовуються для встановлення голосового сеансу зв'язку, а також модемних з'єднань та передачі факсимільних повідомлень.

Під час здійснення телефонного дзвінка підключення між співрозмовниками (абонентами) встановлюється через телефонну станцію виключно з метою організації розмовного з'єднання. Для забезпечення процедур встановлення, підтримки, зміни стану і завершення з'єднання використовується різна телефонна сигналізація, в залежності від типу зв'язку. Під час телефонної розмови голосовий сигнал (слова) перетворюються в електричний сигнал, який передається через телефонну мережу іншій стороні (іншому абоненту). Коли електричний сигнал досягає адресата, він перетворюється в голосовий сигнал оригіналу. Основними перевагами фіксованого телефонного зв'язку є : поширеність, надійність, висока швидкість зв'язку і простота використання.

Інтернет. Мережа Internet – вже давно є своєрідним майданчиком для підготовки та вчинення багатьох видів злочинів.

Проте, співробітники оперативних підрозділів НП України, здійснюючи пошук та фіксацію фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, нерідко використовують різні ресурси мережі Інтернет, не маючи належного уявлення про особливості їх устрою та функціонування, чим значно обмежують можливості оперативного пошуку криміналістично (оперативно) значимої інформації.

Для усунення зазначеного недоліку слід уяснити основні категорії (поняття, терміни, технічні аспекти), що характеризують цю сферу.

Загальне уявлення та технологічні основи функціонування Internet.

Мережа Internet – це глобальна (всесвітня) комп'ютерна мережа, що об'єднує величезну кількість персональних комп'ютерів у різних країнах світу, з'єднаних між собою для спільної роботи. Окремі з комп'ютерів такої мережі підключені на постійній основі і є – *серверами*, інші

підключаються до мережі на деякий час з метою отримання короткочасного доступу до Internet (комп'ютери користувачів).

Технологічні основи функціонування Internet (збереження та передавання даних) мають свої особливості. Так, уся інформація в мережі Internet зберігається у вигляді окремих файлів (сукупність файлів різних типів складає ресурси Internet), які містяться в пам'яті окремої групи комп'ютерів – серверів.

Сервери – це віддалені комп'ютери, які забезпечують роботу серверних програм, що здійснюють оброблення запитів користувачів: їх ідентифікацію, перевірку повноважень, приймання даних від користувачів і передавання їм затребуваних даних. Кожен окремий сервер виступає своєрідним вузлом (розеткою), до якого підключаються інші користувачі. Крім функції підключення користувачів до мережі, такі вузли також можуть зберігати інформацію та передавати її. Кожен сервер має своє унікальне ім'я, а організація чи фізична особа, яка його встановила, має статус сервіс-провайдера.

Сервер провайдера, маючи великий обсяг вільної пам'яті на жорсткому диску, має можливість розділити диск на окремі каталоги, передавши їх в оренду своїм клієнтам за окрему плату. Отримавши доступ до таких каталогів, будь-яка особа може розміщувати на них свою інформацію для загального огляду, стаючи власником – *віртуального серверу.* Програмні можливості такого серверу забезпечують постійне представництво особи в мережі Internet та цілодобовий доступ до завантажених файлів.

Контролювати інформаційний зміст даних, що передаються в мережі, а також підвищувати ефективність її роботи дозволяє *проксі-сервер* – програмний засіб-посередник між локальною і глобальною мережами.

На серверах, що є вузлами мережі, працюють спеціальні програмно-апаратні засоби, які називають *маршрутизаторами*, які забезпечують передавання пакетів інформації між серверами до її адресата.

Обмін даними в мережі Internet здійснюється за допомогою спеціальних протоколів – TCP/IP, BITNET та інших, які задають способи передавання даних, повідомлень, оброблення помилок мережі, забезпечують цілісність та збереженість даних при їх передаванні у середині мережі. Так, Протокол TCP (Transmission Control Protocol) – відповідає за передавання даних, а протокол IP (Internet Protocol) – за їх адресацію.

Для коректної та швидкої передачі інформації вона розбивається на окремі короткі фрагменти (пакети), які послідовно передаються в мережі та на фініші складаються знову в єдине ціле.

Для ідентифікації комп'ютерів, що підключені до мережі Internet використовують унікальні цифрові адреси, які називаються *IP-адресами*[*], що представлені у вигляді запису чотирьох або більше десяткових чисел значенням від 0 до 255, розділених крапками (наприклад, 195.33.22.11 або 155.77.66.1) для того, щоб за допомогою електронних засобів передачі інформації можна було точно вказати куди саме її потрібно доставляти. Крайнє ліве значення запису позначає адресу мережі верхнього рівня, а числа, що стоять праворуч, – більш дрібні ділянки мереж, а останні вказують на конкретний комп'ютер.

[*] У всіх випадках, коли особа підключається до мережі Інтернет, її комп'ютер стає частиною мережі, тому йому має бути привласнена унікальна IP-адреса. Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса щоразу має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення. Статичні IP-адреси, як правило, закріплені за тими вузлами Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів мережі Інтернет.

Аби полегшити розуміння IP-адрес, які є складними для запам'ятовування, і не завжди зручними у використанні, для ідентифікації ділянок мережі використовуються спеціальні назви (*домени).* Імена ділянок мереж, що ієрархічно входять одна в одну, аж до імені конкретного комп'ютера, поєднують в одне загальне ім'я, що визначає IP-адресу конкретного комп'ютера в мережі. Таке ім'я називається *доменним*[*] (також його називають URL-адреса (Uniform Resource Locator), воно складається з двох або більше частин (сегментів), відділених один від одного точками, наприклад www.lduvs.edu.ua. Права частина – «*ua*» відповідає географічному положенню і позначає країну, *«edu»* характеризує форму організації для якої призначається сайт, в даному випадку це державний вищий начальний заклад. Права частина доменного імені називається доменним ім'ям верхнього рівня. Частина доменного імені, розташована ліворуч, часто відповідає назві організації, яка нею володіє. Ця частина доменного імені разом з частиною, що відповідає домену верхнього рівня, називають доменним ім'ям другого або третього рівня. Наприклад, доменне ім'я «*ua*» є доменним ім'ям першого рівня, *edu.ua* – другого рівня, *lduvs.edu.ua* — третього. До доменному імені може також додаватися субдомен – www. Доменні імена мають структуру, зважаючи на котру легко встановити, якій організації належить таке ім'я.

Для знаходження відповідності доменних і IP-адрес була створена спеціальна служба (система доменних імен) – DNS.

Для електронної пошти адреса конкретного користувача складається з двох частин, розділених символом @ (розмовна назва «собачка»), наприклад,

[*] Доменне ім'я – це символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі.

mail@lduvs.edu.ua. Ліва частина «mail» – це ідентифікатор користувача (його ім'я). Права частина «lduvs.edu.ua» – це назва домену серверу, на якому організована поштова скринька.

WWW (*World Wide Web*) – представляє собою єдиний інформаційний простір (всесвітню мережу), що складається із взаємопов'язаних електронних документів, які зберігаються на Web-серверах. Окремі з таких документів, що складають простір Web, називають Web-сторінками, а групи тематично об'єднаних Web-сторінок Web-сайтами (Web-вузлами). Web-сторінки стають доступними для перегляду завдяки спеціальним програмам – браузерам (Browser). Браузер виконує відображення на екрані комп'ютера або мобільного пристрою документів, складених за допомогою мови гіпертекстової розмітки HTML (Hyper Text Markup Language), кожен з яких може містити як внутрішні перехресні посилання, так і посилання на інші документи, що зберігаються на тому ж самому або на будь-якому іншому сервері. Такі посилання називають гіперпосиланнями.

Сукупність гіпертекстових електронних документів, що зберігаються на серверах WWW, утворює своєрідний гіперпростір документів, між якими можливе переміщення. Для здійснення такого переміщення кожен документ у Web-просторі має свою унікальну адресу, яка визначається уніфікованим покажчиком ресурсу URL[8].

Адреса URL будь-якого Web-документу складається з трьох частин:

[8] Див.: Основи інформатики: підручник / укладач: І.О. Яковлева. Харків АПБУ, 2003. С. 154-177; Іванов Г.В. Основи інформатики та обчислювальної техніки: підручник / В.Г. Іванов, В.В. Карасюк, М.В. Гвозденко; за заг. ред. В.Г. Іванова. Харкыв: Право, 2015. С. 225-231, 244-259; Бродський Ю. Б. Обчислювальна техніка та програмування. Ч. І. Інформатика та обчислювальна техніка: навч. посібник / Ю. Б. Бродський, К. В. Молодецька, І. А. Пількевич. Житомир: Вид-во ЖДУ ім. І. Франка, 2014. 204 с.

- ім'я прикладного протоколу, що відповідає службі, яка здійснює доступ до конкретного ресурсу. Для служби WWW прикладним є протокол передавання гіпертексту – http:// (Hyper Text Transfer Protocol);

- указівки доменного імені сервера, на якому зберігається конкретний ресурс, наприклад, http://www.mvs.gov.ua;

- унікального повного шляху доступу до файла на конкретному комп'ютері, наприклад, http://www.mvs.gov.ua/pages/151_evropeyskiy-sud-z-prav-lyudini-.htm.

Де http – це ім'я протоколу, :// – стандартний роздільник, www.mvs.gov.ua – доменне ім'я сервера, pages/151_evropeyskiy-sud-z-prav-lyudini-.htm – шлях пошуку файла Web-документа, www – ім'я комп'ютера в локальній мережі, mvs – ім'я Web-сервера компанії, gov – ім'я домену, якому належить сервер (у даному випадку домен gov – вказує на належність сервера органу державної влади України); ua – позначає країні; pages – позначає перший каталог на комп'ютері WWW; 151_evropeyskiy-sud-z-prav-lyudini-.htm – власне ім'я ресурсу.

Технологічні основи роботи в мережі Internet.

2 грудня 1992 року вважається днем народження українського Internet. Саме в цей день для України було делеговано домен UA.

Станом на початок 2017 року в Україні нараховано 21,6 млн. регулярних користувачів Internet. Проникнення Internet в Україні складає 64,8% (станом на 2011 рік цей показник складав 35%), що свідчить про те, що мережа стала необхідним і невід'ємним засобом розвитку та функціонування суспільства[9].

В основі роботи сучасного Internet лежать такі основні сервіси:

[9] Див.: Semantrum – персональний сервіс моніторингу всіх типів ЗМІ та соцмедіа. URL: https://promo.semantrum. net/uk/2017/04/21/v-ukrayini-na-pochatok-2017-roku-narahovano-21-6-mln-koristuv achiv-internetu/

- *Web-сайти.* Серед різноманітності Web-сайтів вирізняються найбільшою популярністю інтерактивні та багатокористувацькі – *соціальні мережі* та *блоги* (мережеві щоденники) і *Internet-магазини*;

- *пошукові системи.* Для пошуку відомостей в мережі використовуються *пошукові системи* (Google, Yandex – на даний час заблокований, Meta, Ukr.net, Bing та інші), що представляють собою програмно-апаратні комплекси із Web-інтерфейсом (зазвичай це сайти, на яких розміщено інтерфейс системи), що надають можливість пошуку інформації будь-якого роду за ключовими словами;

- *електронна пошта (E-mail). Електронна пошта* представляє собою сервіс мережі Internet, який надає послуги з пересилання й отримання електронних повідомлень та обмін даними будь-якого змісту по розділеній комп'ютерній мережі. Найбільша кількість електронний поштових скриньок відкрита на порталах Google (Gmail), Yandex (Яндекс.Почта), Mail.ru (Почта@mail.ru), Ukr.net (Freemail.ukr.net), I.ua (Пошта@i.ua) та інших. Робота порталів Yandex.ru та Mail.ru на даний час офіційно заборонена та заблокована на території України;

- *Internet-месенджери* – сервіси, що забезпечують можливість обміну електронними повідомленнями між користувачами, які знаходяться в мережі. На даний час найбільш популярними є такі месенджери: Viber, Telegram, WhatsApp, Skipe та інші. Останній месенджер Skipe функціонує за принципом закритого пропрієтарного протоколу, що забезпечує безкоштовний шифрований голосовий та відео зв'язок через Internet між комп'ютерами (VoIP), а також платні послуги зв'язку з абонентами звичайної телефонної або мобільної мережі. Відмінність Skipe від інших програм IP-телефонії полягає у використанні технології P2P (пірінгових мереж), завдяки якій інформація обробляється на комп'ютерах користувачів, що спілкуються, а для її передавання використовується найкоротший шлях. Даний месенджер не

використовує серверів для переадресації і зберігання даних, уся інформація зберігається виключно у самих абонентів, що забезпечує якість зв'язку та повну конфіденційність даних, що передаються. Інші види месенджерів також забезпечують повну захищеність та конфіденційність відомостей, що передаються;

- *сховища файлів* (FTP-сервери), де розміщено файли, доступні для скачування;

- *файлообмінні (пірінгові) мережі** – мережі, що об'єднують користувачів, які мають можливість спілкуватися один з одним та обмінюватися різними файлами (графічними, текстовими, аудіо, відео тощо)[10].

Для початку роботи в мережі необхідно:

- фізично приєднати комп'ютер до одного з вузлів мережі Internet;

- звернутися до провайдера,* укласти відповідний договір на отримання послуг доступу до мережі (в якому вказати свою адресу та персональні дані ПІБ, дані паспорту, контактні номери телефонів) та отримати IP-адресу на постійній або тимчасовій основі;

- встановити і настроїти програмне забезпечення – програми-клієнти тих сервісів, послугами яких користувач мережі має намір скористатися.

В останні роки під час вчинення різних видів злочинів активно використовуються сучасні платіжні засоби,

---

* Пірінгові мережі – однорангові або децентралізовані оверлейні комп'ютерні мережі, засновані на рівноправності учасників. У такій мережі відсутні виділені сервери, а кожен вузол є як клієнтом, так і сервером.

[10] Більш докладно про принципи роботи окремих сервісів мережі див.: Виявлення, документування та розслідування злочинів, передбачених ст. 315 КК України, вчинених з використанням мережі Інтернет: навч.-практ. посібник / В.М. Комарницький, В.О. Криволапчук, Б.І. Бараненко та ін.; МВС України, Луган держу н-т внутр. Справ ім. Е.О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е.О. Дідоренка, 2017. С. 68-88;146-161.

* Провайдер – організація (юридична особа), що надає послуги доступу користувачів до мережі Internet.

такі як електронні гроші та криптовалюти, що також потребує окремого стислого їх розгляду.

«Електронні гроші «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі»[11]. Вони з'явилися як реакція ринку банківських послуг на проблеми безпеки використання платіжних карток та потребу в новому, більш гнучкому, зручному і захищеному платіжному інструменті для оплати товарів та послуг через Інтернет[12]. Цим зумовлюються особливості електронних грошей, які відрізняють їх від безготівкових: електроні гроші не є універсальними і приймаються виключно користувачами відповідних платіжних систем; емісію грошей здійснює виключно Національний Банк України, емісія електронних грошей здійснюється банківськими установами; внаслідок переказу електронних грошей їх одержувач набуває право грошової вимоги до того ж суб'єкта, що й платник; електронні гроші існують в рамках однієї платіжної системи і не здатні до переведення їх в інші платіжні системи у незмінному вигляді[13].

Криптовалюта представляє собою наступний крок у розвитку технологій розрахунків з використанням сучасних інформаційних технологій. Найбільш відомою криптовалютою є Bitcoin. У науковій та популярній літературі представлено достатньо інформації щодо технічних та

[11] Положення про електронні гроші в Україні: Постанова Правління Національного банку України від 04.11.2010 № 481.

[12] Фінансова грамотність: навч. посібник / авт. кол.; за ред. д-ра екон. наук, проф. Т.С. Смовженко. вид. 2-ге, випр. і доп. Київ, 2013. С. 74.

[13] Більш докладно див.: Шимон С. Електронні гроші: форма грошей чи майнові права вимоги?. *Юридична Україна.* 2015. № 9. С. 36–41; Куцевич М., Берзін П. Неправомірний випуск й використання електронних грошей, що вчиняються у системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації). *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* 2013. Вип. 4. С. 13-16.

організаційних особливостей функціонування Bitcoin. Зупинимося на тих, які вважаємо ключовими для відповіді на питання щодо можливостей кримінально-правового регулювання в даній сфері. По-перше, криптовалюта фізично представляє собою певний набір даних згенерований на підставі складного математичного алгоритму. По-друге, платіжна система Bitcoin організована за принципом пірингової мережі (p2p, peartopear – рівний рівному), записи щодо всіх транзакцій розподілені між всіма учасниками системи, єдиний центр координації мережі відсутній, у вільному доступі представлено інформацію щодо всіх здійснених транзакцій. Такий метод організації платіжної системи забезпечує майже абсолютний захист інформації щодо транзакцій, робить систему стабільною та надійною. По-третє, для реєстрації в платіжній системі не використовуються персональні дані, транзакції здійснюються між деперсоніфікованими «електронними гаманцями». По-четверте, Bitcoin – нефіатні гроші, їх вартість нічим не забезпечена і визначається ситуативно на підставі попиту та пропозиції, єдиний орган, що встановлює курс до національних валют, відсутній.

Тим не менше, корисні властивості криптовалюти (захищеність, конфіденційність, децентралізація, майже миттєвий переказ у будь-яку частину світу) забезпечує стабільний попит на неї та стійке зростання курсу до національних валют. Лише з грудня 2016 року по жовтень 2017 вартість Bitcoin зросла з 750 до 5000 доларів США. За таких умов не дивно, що криптовалюта набуває значного поширення в Україні. При цьому Національний банк України (лист від 8 грудня 2014 р. №29-208/72889) розглядає Bitcoin як «грошовий сурогат, який не має забезпечення реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це протирічить нормам українського законодавства». Маємо ситуацію, коли фактично існуючі та динамічні суспільні відносини опиняються

поза межами правового регулювання за умови очевидної необхідності такого. Наприклад, особа вимагає певну суму у Bitcoin або отримує хабар у такій формі. Яким чином встановити ознаки предмета злочину? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідних предметів злочинів? На сьогодні чіткої відповіді на поставлені питання немає. Досвід зарубіжних країн дуже різноманітний, містить приклади від офіційного визнання криптовалюти (Японія, Німеччина) до повного ігнорування. *Очевидно криптовалюти будуть дедалі частіше використовуватися в злочинній діяльності.* За таких умов найбільш доцільно сформулювати прості та прозорі правила для сфери кримінально-правового регулювання, зокрема передбачити механізм оцінки. Представлення у процесуальній формі даних про криптовалюти створить нові умови для якісного оновлення діяльності правоохоронців. Виникнуть принципово нові види тактичних операцій, що збільшить можливості протидії злочинності. Варто зазначити, що ці питання слід розглядати як складові більш загальної проблеми – можливості використання технологій Big Data у правоохоронній діяльності[14]».

Знання основних положень побудови та функціонування мобільного та фіксованого зв'язку, а також мережі

[14] Карчевський М.В. Можливості Big Data та кримінально-правова комунікація. *Матеріали Міжнародної науково-практичної конференції «Політика в сфері боротьби зі злочинністю»*. Івано-Франківськ, 2017. С. 52-58; Карчевський М.В. Особливості кримінально-правової кваліфікації злочинів проти власності, що вчиняються з використанням комп'ютерної техніки. *Діяльність підрозділів карного розшуку Національної поліції України щодо протидії злочинам проти власності, особливо корисливо-насильницьким у сучасних умовах*: збірн. матер. постійн. діюч. семінару (м. Миколаїв, 1-3 червня 2017 р.); за ред.: д.ю.н., проф. В.М. Комарницького, к.ю.н., доц. С.А. Комісарова, к.ю.н., проф. Б.І. Бараненка. Сєвєродонецьк: Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка, 2017. С. 18-19; Бочковий О.В. Блокчейн відкритого суспільства, або реальні здобутки віртуального середовища. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. № 2. С. 69-77.

Internet, роботи їх основних сервісів дозволить працівникам оперативних підрозділів Національної поліції України підвищити власну компетентність у володінні мобільною та комп'ютерною технікою, краще орієнтуватися у методах пошуку, оброблення та аналізу інформації, яка знаходиться у операторів та провайдерів телекомунікацій, розміщена в мережі, надасть можливість більш ефективно і змістовно застосовувати отримані в такий спосіб відомості у протидії злочинам.

РОЗДІЛ 2
ОСОБЛИВОСТІ ВЧИНЕННЯ ЗЛОЧИНІВ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НА ПРИКЛАДІ НЕЗАКОННОГО ЗБУТУ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН, ЇХ АНАЛОГІВ АБО ПРЕКУРСОРІВ БЕЗКОНТАКТНИМ СПОСОБОМ

Незаконний збут наркотичних засобів, психотропних речовин, аналогів або прекурсорів – це будь-які оплатні чи безоплатні форми їх відчуження всупереч вимогам законодавства. Серед таких форм: продаж, дарування, обмін, сплата боргу, оплата виконання робіт чи надання послуг, введення володільцем цих засобів або речовин ін'єкцій іншій особі за її згодою (*однак обопільне введення ін'єкцій наркотичного засобу, психотропної речовини чи їх аналога особами, які придбали їх за спільні гроші, збуту не утворюють*), пропозиція викурити цигарку, яка містить вказані речовини. В останньому випадку дії особи потрібно кваліфікувати за сукупністю кримінальних правопорушень, передбачених ст. 307 та ст. 315 КК України.

Якщо відповідні засоби або речовини збуваються чи передаються в місця позбавлення волі, вчинені дії утворюють кваліфікований склад кримінального правопорушення й кваліфікуються за ч. 2 ст. 307 КК України. Виділяють чотири найбільш поширених способи незаконного збуту:

1) *відкритий контактний* (безпосередній та особистий збут наркотичної речовини, що здійснюється способом: обміну; на умовах позики; дарування; безоплатної передачі; передачі наркотичних засобів за надання певних послуг; введення ін'єкції однією особою іншій);

2) *відкритий опосередкований* (посередницький), за якого ланцюг «продавець – покупець» розривається одним або декількома посередниками (наркотичний засіб і гроші передаються через посередника);

3) *замаскований контактний* (передача наркотичних засобів і грошей під виглядом передавання будь-яких речей: газети, книжки, іграшки тощо);

4) *безконтактний* (віддалений або дистанційний)[15] – повідомлення про місце зберігання наркотичних засобів покупцеві, у тому числі закладки наркотичного засобу в обумовленому з покупцем місці (закладці) здійснюється після попереднього замовлення певного наркотичного засобу (наприклад, за допомогою мобільного зв'язку) та віддаленої оплати (за допомогою електронних платіжних систем, електронних грошей тощо).

Саме під час незаконного збуту «безконтактним способом»* наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (а це стосується і зброї, боєприпасів та інших предметів, обіг яких заборонено чи в окремих випадках обмежено), злочинцями для контактів між постачальниками та покупцями та з метою усклад-

[15] Див.: Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. 9-те вид., переробл. та допов. Київ: Юридична думка, 2012. С. 904; Про судову практику в справах про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: Постанова Пленуму Верховного Суду України від 26 квітня 2002 року № 4 (зі змінами, внесеними постановою від 18.12.2009 № 16). URL: http://www.scourt.gov.ua/clients/vs.nsf; Гогов Р.А. Методика расследования преступлений, связанных с незаконным оборотом наркотических средств, совершаемых организованными группами: дис... канд. юрид. наук: 12.00.09. Москва, 2010. С. 244; Ошлыкова Е.А. Методика расследования незаконного сбыта наркотических средств и поддержания государственного обвинения по уголовным делам данной категории: монография. Москва: Юрлитинформ, 2013. С. 21-31; Прокопенко Н.М. Криміналістична характеристика та основні положення розслідування незаконного збуту наркотиків: дис. канд. юрид. наук: 12.00.09. Харків, 2014. С. 47-51.

* Під час «Безконтактного» (дистанційного) збуту – між «продавцем» та «покупцем» виключений будь-який фізичний контакт.

нення контролю з боку правоохоронних органів найчастіше застосовуються сучасні інформаційно-телекомунікаційні та інші технології (мобільний зв'язок, ресурси мережі Інтернет, IP-телефонія, динамічні IP-адреси, різні програми шифрування та миттєвого обміну повідомленнями тощо), що знижують ризик викриття протиправної діяльності (суттєво ускладнюють використання співробітниками оперативних підрозділів класичних (традиційних) методів виявлення та документування таких злочинів), дозволяють діяти завуальовано, мінімально ідентифікуючи себе. Указані обставини потребують додаткового висвітлення.

Типову схему незаконного збуту наркотичних засобів безконтактним способом складають такі дії:

1. Пошук покупцем інформації про незаконний збут (продаж) наркотичних засобів. Відомості про доступні для придбання види наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів зашифровані за допомогою умовних термінів (сленгові назви, специфічні вирази, що мають відношення до обігу наркотичних засобів), а також контакти для зв'язку із особами, які здійснюють їх незаконний збут (номери мобільного телефону, адреси електронної пошти, логіни для зв'язку за допомогою Skipe або Інтернет месенджерів), зазвичай поширюються шляхом:

а) нанесення відповідних надписів на стінах будівель, парканах, асфальті і т.ін. Це так звана зовнішня («настінна», «асфальтова» тощо) реклама наркотичних засобів, яка найчастіше являє собою виконані фарбою надписи із зазначенням ключових слів, що вказують на характер товару, який реалізується (сіль, просочення, мікс тощо) та контактних даних збувальників (номер ICQ або мобільного телефону, логін користувача Skype чи особи диспетчера, адреса електронної пошти, назва сайту).

Надписи можуть виконуватись як від руки, так і з використанням спеціально виготовлених трафаретів, що прискорюють їх нанесення.

Способи зовнішньої реклами вдосконалюють з урахуванням технічної грамотності потенційних покупців та належності їх до неформальних молодіжних груп з яскраво вираженою субкультурою. Зокрема, замість надписів фарбою, що безпосередньо вказують на вид незаконного товару, який пропонується для придбання, можуть використовуватися невеликі фрагменти самоклеючого паперу або полімерної плівки (стікери) з нанесеною на них інформацією про розповсюджувачів наркотичних засобів з вказівкою номерів ICQ та телефонів, Інтернет-адрес та інших контактних даних у вигляді QR-кодів.

Указані стікери можуть розміщуватись у будь-якому людному місці, наприклад, на стінах підземних переходів, огорожах, парканах, дошках оголошень у під'їздах і ін. Для маскування стікери з QR-кодом можуть наклеювати поверх уже наявних рекламних оголошень та іншої продукції, розміщеної в спеціально відведених для цього місцях. Такий спосіб розповсюдження наркотичних засобів не несе прямої візуальної вказівки на збут наркотичних засобів, не викликає негативної реакції в населення з огляду на неможливість прочитати QR-код без застосування спеціального програмного забезпечення. Водночас у мережі Інтернет міститься значна кількість програм перекладу текстової інформації в QR-код та назад. Зацікавлена особа може прочитати закодовану інформацію, володіючи навіть базовою моделлю смартфона, яка має утиліти (програмні додатки) для розпізнавання QR-кодів (наприклад, «QR droid» – Android, «RedLaser» – iOS, «QR Code Scanner Pro» – Blackberry). Ще одним способом вуличної реклами наркотичних засобів та їх аналогів можуть бути графіті, нанесені на стіни та паркани. Незрозумілі для більшої частини населення «хитромудрим» спо-

собом переплетені малюнки та надписи, будучи елементом вуличної субкультури, можуть нести змістовне навантаження для певної категорії громадян, інформуючи їх про розповсюджувачів наркотичних засобів;

б) поширення таких відомостей:

- різними способами в мережі Інтернет (у соціальних мережах, на спеціально створених веб-сайтах);
- серед знайомих та наркозалежних осіб.

Відповідно, безкарність вчинення таких дій, відносна доступність і уявна безпека формують у здорового населення, в першу чергу, молоді, уявлення про те, що такі речовини є легальними, а їх поширення і вживання не є протизаконним.

2. Встановлення контакту з особою, що здійснює незаконний збут, замовлення наркотичного засобу, узгодження деталей незаконної оборудки. У переважній більшості випадків контакт зі збувальником встановлюється:

- *шляхом здійснення телефонного дзвінка* на заздалегідь відомий номер (номер, який повідомили знайомі, наркозалежні особи або номер, розміщений на стіні, паркані), номер розміщений на сайті в мережі Інтернет, що складає – у 47% від усіх досліджених випадків. З них 42% комунікацій відбувалася виключно в телефонному режимі, а в одиноких випадках телефонні контакти додатково супроводжувалися отриманням замовником SMS-повідомлення про місце закладки наркотичного засобу (4%) або отриманням такого ж повідомлення в соціальній мережі Вконтакте (1%);
- трохи більше аналогічних контактів (43%) здійснювалося *через мережу Інтернет*. При цьому також у рідких випадках узгодження деталей оборудки додатково супроводжувалося контактами у соціальних мережах та відправленням SMS-повідомлень. Виявлені також рідкісні випадки (2%) пересилання через мережу Інтернет на мобільний телефон замовника фотографії з місцем (кар-

тою місця) розташування закладки з наркотичною речовиною; замовлення наркозасобу через сайт у мережі Інтернет та отримання повідомлення щодо місця організації закладки через програмне забезпечення для шифрованого голосового зв'язку Skype (2%). В значній кількості випадків контакти з метою замовлення та стосовно збуту наркозасобів відбувалися через мережу Інтернет і соціальні мережі з наступним відправленням SMS-повідомлення, обміном телефонними номерами і контактуванням у телефонному режимі:

1) *узгодження деталей оборудки та оплати під час особистої зустрічі* з повідомленням місця закладки – 10 % випадків;

2) *шляхом відправлення повідомлення на електронну пошту* – у 2 % випадків.

3. Оплата за замовлений наркотичний засіб. Найбільш розповсюдженими способами оплати за замовлений наркотичний засіб були такі:

- переказ грошей з банківської картки на картку або поповнення рахунку картки у відділенні банку, в системі самообслуговування або через термінали оплати;
- банківський переказ грошей конкретній особі, що не потребує відкриття окремого рахунку;
- поповнення рахунку мобільного номеру з подальшою конвертацією та переказом отриманої суми на банківську картку (таку послугу надає ПрАТ «Київстар»);
- перерахування електронних грошей* (e-money) на рахунок (електронний гаманець) злочинця. Станом на 1 січня 2018 року НБУ надав право здійснювати випуск та інші операції з такими електронними грошима:

* Електронні гроші (e-money) – одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі. URL: https://bank.gov.ua/control/uk/publish/article?art_id=123302

«FORPOST» (ПАТ «Альфа-Банк»); «Максі» (АТ «ТАСкомбанк»); «ГлобалМані» (ПАТ КБ «Глобус»); «Електрум» (АБ «Укргазбанк»); «MasterCard» (ПАТ «Банк Восток», ПАТ «Альфа-Банк», АТ «ТАСкомбанк», ПАТ КБ «Приватбанк», ПАТ «ПУМБ»); «Visa» (ПАТ «Укрсоцбанк», АТ «Ощадбанк», ПАТ «ПУМБ»); «ПРОСТІР» (АБ «Укргазбанк», ПАТ «Юнекс Банк»);

- перерахування криптовалюти, наприклад, Bitcoin*;
- передання грошей особисто в руки під час зустрічі;
- шляхом залишення грошових коштів в обумовленому місці, у тому числі під час отримання наркозасобу на місці залишеної закладки.

Як свідчать результати узагальнення, майже у 90% випадків оплата за наркотичний засіб здійснюється способами, які виключають безпосередню особисту зустріч та візуальний контакт між збувачем та покупцем, що підвищує конспіративність даного виду незаконної діяльності та ускладнює роботу працівників оперативних підрозділів по їх встановленню та документуванні протиправної діяльності.

Повідомлення замовнику відомостей про місце організації закладки. Аналіз кримінальних проваджень та обвинувальних вироків суддів України вказують на те, що місцями організації закладок наркотичних засобів найчастіше були такі місця:

1) *на вулиці біля будинку (приватного домоволодіння)* – 17 % випадків;

2) *на вулиці біля багатоквартирного будинку* (в стіні арки будинку; під адресною табличкою будинку; під балконом будинку; на підвіконні вікна поблизу від таблички з номером будинку; на розі будинку; біля номеру будинку; біля паркану будинку; біля підвального приміщення; за дошкою об'яв, зліва від вхідних дверей до

* У м. Києві з вересня 2017 року почали встановлювати платіжні термінали самообслуговування з можливістю придбання криптовалют.

під'їзду будинку; на даху підвального приміщення будинку; під планкою підвіконня першого поверху праворуч від вхідної двері під'їзду; у отворі вентиляції підвалу біля під'їзду будинку; у правому дальньому куті будинку під балконом ліворуч від вхідної двері під'їзду) – 15 % випадків;

3) *випадково обрані місця* (в лівій кишені куртки, яка висіла на дереві в лісопосадці; на землі біля сміттєвого баку; на вулиці на землі; на землі біля школи; на землі в парку; на землі в районі площі; на землі вздовж автодороги; на землі біля Собору; на землі біля автостанції; на землі біля кафе; на асфальті автомобільної траси між містами – 9 % випадків;

4) *під лавкою (на лавці), що знаходилася*: біля будинку; біля паркану будинку; неподалік будинку; неподалік під'їзду будинку; біля під'їзду будинку на землі; у парку – 6 % випадків;

5) *біля стовпа електромережі* поруч з будинком (під стовпом лінії електропередач біля будинку; під опорою лінії електропередач по вулиці; під ліхтарним стовпом біля будинку; біля ліхтарного стовпа на землі) 5 % випадків;

6) *біля під'їзду будинку на землі* – 5 % випадків;

7) *в під'їзді багатоквартирного будинку* (між першим та другим поверхом праворуч від сходів; під сходами; за поштовою скринькою квартири; у поштовій скриньці; на магніті ящика Інтернету) – 5 % випадків;

8) *біля станції метро* – 4 % випадків;

9) *на вулиці на землі* – 4 % випадків;

10) *під деревом* (з торця будинку; в лісопосадці; навпроти будівлі школи; на землі; біля дерева) – 4 % випадків;

11) *на зупинці громадського транспорту* (на сидінні, в гумовій шині, на землі) – 3 % випадків;

12) *в клумбі біля під'їзду будинку* (біля магазину, на заправці) – 3 % випадків;

13) *на вулиці поблизу супермаркету* (біля супермаркету; біля магазину; за приміщенням магазину) – 3 % випадків;

14) *під дорожнім знаком* «Пішохідний перехід» біля будинку (біля дерева; біля дорожнього знаку початок населеного пункту на узбіччі дороги) – 3 % випадків;

15) *відділення служби доставки* (ТОВ ТД «Міст Експрес», «Нова пошта») – 2 % випадків;

16) *між гаражами* (біля будинку, біля гаражу) – 2 % випадків;

17) *прибудинкова територія* (приватного домоволодіння; біля приватного домоволодіння; покинутого домоволодіння) – 2 % випадків;

18) *територія* (автозаправної станції, фруктового саду поблизу СТО, дитячої площадки) – 2 % випадків;

19) *під колесом біля будинку; в шині у парку; в гумовому колесі напроти будівлі дитячого садка* – 2 % випадків;

20) *під мостом* (неподалік від зупинки громадського транспорту; на землі) – 2 % випадків;

21) *у кущах* – 2 % випадків;

22) *місця, вказані збувальником при вивезенні кліента на місце організації закладки* – 1 % випадків.

Серед наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, найбільш поширених в якості предмета закладки були:

1) опій та опій ацетильований – 32 % випадків;
2) метадон – 28 % випадків;
3) амфетамін – 22 % випадків;
4) канабіс – 5 % випадків;
5) героїн (в окремих випадках героїн збувався із кокаїном та метадоном) – 4 % випадків;
6) концентрат із макової соломи (в окремих випадках із прекурсором ангідридом оцтової кислоти) – 3 % випадків;
7) меткатиноном (ефедрон) – 1 % випадків;
8) PVP – 1 % випадків;

9) 2 (Pyrralidih-1-y) -1-(fhiophen-2-y)) pertan-arie (-PVT); 4 бром-2,5- диметоксиамфетамін (ДОВ); 5-Fluoro-AB PINACA – 1 % випадків;

10) MPHP (гомолог речовини MPBP), AB-PINACA-CHM, PVP – 1 % випадків;

11) марихуана – 1 % випадків;

12) таблетки «екстазі», які містять у своєму складі особо небезпечну психотропну речовину МДМА – 1 % випадків.

Зазначені вище наркотичні засоби, психотропні речовини, їх аналоги або прекурсори *на момент безконтактного збуту були упаковані наступним чином:*

1) амфетамін – у згортки (з паперу, поліетилену, фольги, банкнот Національного Банку України різного номіналу); поліетиленові пакети; пачки з під цигарок;

2) метадон – у згортки (з паперу (газет), поліетилену, фольги); поліетиленові пакети; пачки з під цигарок; медичні шприци;

3) опій, опій ацетильований та концентрат з макової соломи – у ін'єкційні медичні шприци одноразового застосування (які збуваються без камуфляжу, закамуфльовані в картонні коробки, пачки з під цигарок, поліетиленові пакети); латексні вироби (презервативи), у тому числі, закамуфльовані у пачки з-під цигарок; флакони, скляні колби;

4) канабіс, героїн та кокаїн – у згортки (з паперу, поліетилену, фольги), у тому числі, закамуфльовані у пачки з під цигарок, соку; поліетиленові пакети;

5) речовини PVP; 2 (Pyrralidih-1-y) -1-(fhiophen-2-y)) pertan-arie (-PVT); 4 бром-2,5- диметоксиамфетамін (ДОВ); 5-Fluoro-AB PINACA; марихуана; таблетки «екстазі», які містять у своєму складі особо небезпечну психотропну речовину МДМА – у згортки, переважно з паперу;

6) героїн; MPHP (гомолог речовини MPBP), AB-PINACA-CHM, PVP – 1 % випадків; меткатиноном (ефедрон) – у полімерні пакети;

При вчиненні збуту наркотичних засобів безконтактним способом зазвичай задіяні такі учасники:

- *диспетчер* – особа, яка отримує замовлення від споживачів наркотичних засобів, передає інформацію особі, яка організовує закладку (закладникові), контролює надходження оплати, отримує адреси місць організації закладок наркотичних засобів від закладників та відправляє адреси каналами зв'язку споживачам;

- *закладник* – особа, яка за вказівкою диспетчера поміщає наркотичний засіб у певне місце, адресу якого надсилає диспетчерові;

- *кур'єр* – особа, яка відповідає за фасування наркотичного засобу та поповнення його кількості в закладників;

- *касир* – особа, яка знімає грошові кошти, отримані через платіжні термінали, з банківських рахунків та розподіляє їх між певними членами групи або передає організаторові групи.

Результати аналізу спеціальної літератури та слідчої практики показали, що безконтактний збут наркотичних засобів організований зазвичай таким способом. На створеному злочинцями ресурсі в мережі Інтернет розміщується реклама пропонованих для реалізації наркотичних засобів (форма подачі матеріалу може бути завуальованою). Тут же вказуються способи оплати «товару». Споживачеві пропонується відправити замовлення з зазначенням виду та кількості речовини, яку він бажає придбати, з використанням SMS-повідомлень, Інтернет-месенджерів, електронної пошти або через ресурси соціальних мереж. При отриманні замовлення один з учасників злочинної групи, який виконує функції диспетчера Call-центру, надсилає повідомлення-відповідь покупцеві з вказівкою суми та способу сплати, яку може бути здійснено через електронні платіжні системи (Webmoney, QIWI тощо) або через пересилання кодів карт сплати послуг мобільного зв'язку. Після здійснення платіжної транзакції покупцеві відсилається повідомлення з інформацією про

місце знаходження схованки з наркотиками. В окремих випадках після сплати грошей злочинці надсилають покупцеві посилку з придбаною речовиною поштою або кур'єрськими службами на адресу, зазначену в заявці.

Деякі Інтернет-магазини застосовують практику використання зацікавленими особами спеціальних програмних алгоритмів для автоматичного (покрокового) замовлення наркотиків. Суть указаних сервісів полягає в тому, що покупець не листується з людиною-оператором, а виконує вказівки програми, поетапно обираючи потрібні речовини, формує «кошик» замовлення, вносить платню на вказаний рахунок, після чого знайомиться з інформацією про порядок отримання наркотичного засобу. Особи, які незаконно розповсюджують наркотичні засоби за допомогою мережі Інтернет та використовуючи канали зв'язку, у процесі протиправної діяльності формують клієнтську базу з контактними даними осіб, які зверталися до них з метою придбання вказаних речовин (номери мобільних телефонів, електронна пошта, ICQ, Skype та інші відомості), яка у випадку блокування роботи сайту дозволяє наркозбувальникам зберегти зв'язок з клієнтами, інформувати їх доступними каналами зв'язку про нове місце знаходження (адресу) Інтернет-сайту[16].

Організовуючи незаконний збут наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів і використовуючи з цією метою можливості мережі Інтернет, злочинці нерідко застосовують спеціальні прийоми (програмне забезпечення), які приховують інформацію про фактичні адреси їх мережевої активності, дозволя-

[16] Кривонос М.В., Бондар В.С. Теорія та практика використання спеціальних знань в розслідуванні злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: монографія; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е. О. Дідоренка, 2017. С. 131-135.

ючи вчиняти протиправні дії в мережі Інтернет на умовах анонімності, а мережеві ресурси створюють на серверах, розміщених у різних країнах.

Так, широко розповсюджене програмне забезпечення, наприклад, Tor (The Onion Router), VPN Master та ін. через мережу проміжних комп'ютерних засобів, які належать користувачам мережі в інших країнах, забезпечує анонімність користувача в мережі Інтернет, захищає його від аналізу та прослуховування трафіку, приховує IP-адресу використовуваного технічного пристрою та, відповідно, його фізичне місцерозташування. Названі властивості досягаються за рахунок багаторівневого шифрування трафіку, що передається для декількох довільно обраних вузлів мережі Tor та послідовної трансляції через ці вузли до користувача. Є очевидним, що функціональні можливості програмного забезпечення Tor та йому подібних програмних продуктів позбавляє представників правоохоронних органів можливості виявляти віртуальні сліди, які утворюються злочинцями при використанні ресурсів мережі Інтернет.

Здійснення слідчих (розшукових) дій та негласних слідчих (розшукових) дій щодо доступу до таких комп'ютерів може викликати ускладнення, оскільки обчислювальна система знаходиться в межах юрисдикції іншої держави. У таких випадках для виявлення злочину нерідко є потрібним використання складних механізмів взаємодії правоохоронних органів різних держав. Усе це призводить до ускладнення в міжнародному масштабі правових та технічних проблем, пов'язаних з виявленням та ідентифікацією злочинців. Звичайно, ефективне реагування на злочинні дії вказаних формувань неможливе без певного коригування його методів. Основне завдання полягає в тому, щоб за виявленими на мережевих ресурсах відомостями про злочинну діяльність із розповсюдження наркотичних засобів встановити

джерело протиправної активності та його місце розташування. За таких умов суттєво підвищується роль засобів спеціальної оперативної техніки.

Це дозволяє мати доступ до інформації, яка передається в з'єднанні та (або) повідомленні електрозв'язку абонентів, інформації про місцезнаходження радіоелектронного засобу, відносно якого проводиться НС(Р)Д; встановлювати постійну IP-адресу, IP-адресу, яка встановлюється по масці, ім'я облікового запису користувача, яке використовується для ідентифікації користувача послуг зв'язку при доступі до мережі передачі даних та телематичним послугам зв'язку, електронну поштову адресу сервісів, які не використовують засоби захисту інформації, включаючи криптографічні, телефонний номер користувача (того, який визивається та (або) того, який визиває), ідентифікатор абонентської телефонної лінії, який використовується для ідентифікації користувача послуг зв'язку при доступі до мережі передачі даних та телематичним послугам зв'язку з передачі даних для цілей передачі голосової інформації, міжнародний ідентифікатор абонента мережі рухомого зв'язку (IMSI), міжнародний ідентифікатор мобільного обладнання (IMEI), унікальний ідентифікатор обладнання мереж передачі даних (MAC-адресу), ідентифікатор служб обміну повідомленнями (включаючи ICQ), мобільний ідентифікаційний номер мобільної абонентської радіостанції (MIN) тощо.

На початковому етапі виявлення розглядуваного виду злочинів особливого значення набуває пошук первинної інформації в мережі Інтернет та її перевірка, проведення яких передбачає наявність в оперативного співробітника спеціальних знань та вмінь. Для виявлення інформації насамперед використовується пошук за інформаційними ресурсами Інтернет із застосуванням різного роду пошукових систем (типу Google, Meta тощо). У процесі виявля-

ються сайти, пов'язані зі злочинними організаціями, а також інформаційні ресурси, що містять заборонену до розповсюдження інформацію.

За результатами пошуку вживаються заходи зі встановлення осіб організаторів таких сайтів. Проте використання лише такого підходу не може забезпечити достатньої ефективності інформаційного пошуку в кіберпросторі, оскільки в ньому існують великі закриті для пошукових серверів зони, які можуть використовуватися з деструктивною метою (зокрема й для розповсюдження наркотичних засобів, зброї). Одним з перспективних напрямів інформаційного пошуку в мережевому інформаційному просторі став Інтернет-моніторинг, що являє собою комплексну систему спостереження за станом кримінальних проявів у мережевому соціальному середовищі, спрямовану на збір, оброблення та аналіз інформації про явища кримінального змісту. Основні напрями цього моніторингу, що здатні забезпечити високу інтенсивність надходження криміналістично значущої інформації такі:

а) автоматизований пошук мережевих інформаційних ресурсів, що містять заборонену до розповсюдження інформацію;

б) вивчення виявлених мережевих ресурсів, пов'язаних з діяльністю злочинних груп;

в) спостереження за закритими для загального доступу місцями мережевого спілкування кримінальної спрямованості.

Після виявлення ресурсів, через які організовано збут наркотичних засобів, зброї важливо забезпечити встановлення контакту з продавцями (диспетчером), способів зв'язку з ними та особистих даних, серед яких номери мобільних телефонів, електронних гаманців, банківських рахунків тощо. Наведення довідок та застосування спеціальних заходів дозволяє встановити осіб, на яких зареєстровані банківські рахунки, зібрати максимальну кількість особистісної інформації тощо.

Важливо вжити заходів до визначення фізичного місцезнаходження пристроїв, за допомогою яких злочинці здійснюють вихід у мережу Інтернет, а також їх MAC-адреси. Подальші дії пов'язані із застосуванням усього комплексу засобів та методів, що підтвердили ефективність у протидії наркозлочинності[17].

Крім зазначеного, провину осіб, причетних до незаконного збуту наркотичних засобів та інших предметів, обіг яких заборонено, може бути також доведено:

– результатами дослідження способів передавання протиправного контенту (електронною поштою, записами на диски чи флеш-картки пам'яті);

– результатами відстеження обміну інформацією через мережу Інтернет, які здійснював підозрюваний;

– зв'язком підозрюваного з роботою на певному комп'ютері, на якому здійснювалося наповнення вебсайту інформацією протиправного характеру та незаконний збут наркотичних засобів та інших предметів;

– результатами дослідження змісту жорсткого диску з комп'ютера підозрюваного та потерпілого зі слідами журналів роботи в мережі Інтернет (закладки, пошукові запити), тимчасових файлів (кеш, Cookie-файли, буфер друку, місце зберігання інформації, записаної на комп'ютер веб-сайтом), змісту своп-файлу «вільне місце», списків друзів + особистих профілів + записів чат-кімнат + інших збережень «області»; відстеженням дат збере-

[17] Див.: Ишин А.М. Современные проблемы использование сети Интернет в расследовании преступлений. *Вестник Балтийского федерального университета им. И. Канта*. 2013. Вып. 9. С. 116-123; Поляков В.В., Кондратьев М.В. Криминалистические особенности бесконтактного способа совершения наркопреступлений. *Известия Алтайского государственного университета.* № 2 (86). Том. 1. 2015. С. 83-86; Шебалин А.В. Особенности этапа предварительной проверки материалов о незаконном сбыте наркотических средств, совершённым бесконтактным способом. *Актуальные проблемы борьбы с преступлениями и иными правонарушениями*: материалы тринадцатой международной научно-практической конференции. часть 1. 2015. С. 150-154.

ження файлів (у файлі Windows зберігаються дати створення (коли файл було створено), останнього запису (коли файл востаннє було змінено) та останнього доступу до файлу (коли файл востаннє було відкрито);

– іншими документами, що свідчать (підтверджують) протиправні дії особи[18]..

[18] Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рекомендації / О.Ф. Вакуленко, О.М. Стрільців, О.С. Тарасенко та ін. Київ, 2016. С. 25-26.

РОЗІДЛ 3
ПРОЦЕСУАЛЬНИЙ ПОРЯДОК ФІКСАЦІЇ ПРОТИПРАВНОЇ ІНФОРМАЦІЇ, РОЗМІЩЕНОЇ В МЕРЕЖІ ІНТЕРНЕТ

Основною метою фіксації інформації про підготовку або вчинення злочинів із використанням інформаційно-телекомунікаційних технологій (наприклад, незаконного обігу наркотичних засобів або зброї, відомості про які розміщені на веб-сайтах, як то форумах, блогах тощо в мережі Інтернет) є документальна фіксація (отримання належних і допустимих доказів) незаконних дій та причетності до них конкретної особи (групи осіб).

Можна виділити два основні способи фіксації таких даних:

- *візуальний*, пов'язаний із зовнішнім сприйняттям (візуальним* оглядом) інформації, розміщеної на веб ресурсі, яка подається на пристрій виведення інформації (монітор));
- *технологічний*, пов'язаний із застосуванням можливостей спеціального програмного забезпечення для фіксації даних[1].

Як правило при фіксації (закріпленні) інформації у мережі такі способи застосовуються одночасно та в комплексі.

До основних форм фіксації (закріплення) інформації протиправного характеру в мережі Інтернет можна віднести наступні:

---

* Візуальний – який здійснюється безпосередньо очима.

[1] Див.: Зеров К.О. Фіксація змісту веб-сторінки в мережі Інтернет як елемент здійснення права на захист авторських прав на твори, розміщені в мережі Інтернет. *Адвокат.* 2015. № 2. С. 18.

а) складання ініціативного рапорту працівником оперативного підрозділу про факт виявлення незаконного обігу наркотичних засобів, вогнепальної зброї або інших предметів на конкретному веб-сайті (ресурсі) в мережі Інтернет;

б) складання текстового документу з копіюванням посилання на конкретну сторінку веб-сайту та наявної на ній фактичної інформації для можливості її перегляду в режимі «оффлайн»;

в) знімок сторінки веб-сайту з екрану (скріншот або Web-скріншот) за допомогою спеціальних програм (наприклад, screenweb, web-capture, full page screen capture, screenshotmachine та ін.) або клавіші «*PrtSc*» та вставки у редактор зображень ***«Paint»*** з подальшим її друком за допомогою периферійних друкувальний пристроїв (принтерів);

г) повноцінна копія сторінки веб-сайту за допомогою спеціальних програм та її збереження на носій інформації. За такої форми закріплення здійснюється фіксація не тільки візуального відображення, а й вихідного коду, URL-адреси веб-сторінки та часу здійснення такої фіксації. Різновидом цього способу є фіксація за допомогою приватних онлайн-сервісів кешованої копії веб-сторінки у пошукових системах. Якщо з моменту видалення веб-сторінки минуло небагато часу, існує шанс, що вона була збережена у вигляді кешованої копії веб-сторінки, зафіксованою відповідною пошуковою системою у момент, коли пошукова система веб-браузеру востаннє відвідувала зазначену веб-сторінку[1];

д) отримання довідки від провайдера, який надає послуги доступу до мережі Інтернет. Така довідка може містити інформацію щодо дій користувачів з приводу розміщення інформації;

[1] Див.: Жуковський Т. Фіксування контенту веб-сторінки як доказу в судовому процесі. *Юридична практика.* 2013. № 39. С. 41.

є) складання протоколу слідчого огляду веб-сторінки з повною фіксацією інформації протиправного характеру, яку вона містить[1]. Такий огляд здійснюється шляхом безпосереднього сприйняття слідчим, прокурором інформації, розміщеної на веб-сторінці за допомогою службового комп'ютера з доступом до мережі Інтернет. У протоколі огляду слід зазначити серійний номер службового комп'ютера, назву та версію встановленої операційної системи, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет. Веб-сторінка має бути масштабована на повний розмір (100%). У браузері мають бути відключені усі додатки, що можуть змінити вигляд веб-сторінки, яка оглядається.

Під час огляду у протоколі фіксуються основні реквізити веб-сторінки, а саме: адреса у мережі Інтернет, на якій розміщено веб-сторінку; назва веб-сайту, категорія оголошення, якщо воно зазначено на веб-сторінці; назва оголошення; основний його текст; прикріплені зображення та аудіо- чи відеофайли; відомості про автора оголошення (якщо воно не є анонімним). У протоколі також має бути перелічено та коротко описано фото-, відео- та аудіофайли, прикріплені до оголошення, із зазначенням посилання на кожний із таких файлів у мережі Інтернет.

Більшість веб-сайтів в мережі Інтернет дозволяють користувачам коментувати опубліковані в мережі повідомлення. Виходячи з цього, вчені рекомендують практичним працівникам досліджувати зміст та час публікації таких коментарів, з метою виявлення осіб, яких цікавить протиправний зміст оголошень та які можуть бути причетні до вчинення таких злочинів. Після огляду

[1] Див.: Виявлення, документування та розслідування злочинів, передбачених ст. 315 КК України, вчинених з використанням мережі Інтернет: навч.-практ. посібник / В.М. Комарницький, В.О. Криволапчук, Б.І. Бараненко та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е. О. Дідоренка, 2017. 505 с.

веб-сторінку необхідно роздрукувати за допомогою службового принтера та додати до протоколу огляду в якості додатка, із зазначенням серійного номера, назви та моделі принтера. Фото-, відео- та аудіо-файли, що є частиною оголошення, також мають бути збережені та записані на диск, який долучається до протоколу огляду в якості додатку[1];

е) проведення безперервної відеофіксації процесу дослідження конкретної веб-сторінки та її змісту;

з) проведення фіксації і дослідження змісту веб-сторінки у мережі Інтернет в рамках платних послуг, які надають Український Мережевий Інформаційний Центр та Центр компетенції українського сегменту мережі Інтернет.

[1] Див.: Коваленко А.В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України.* № 1 (88) 2017. С. 187-188.

РОЗДІЛ 4
ЗМІСТ ТА ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ ПРО АБОНЕНТА ТА НАДАНІ ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ, ЯКА ЗНАХОДИТЬСЯ В ОПЕРАТОРІВ ТА ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ

Враховуючи стрімкий розвиток телекомунікаційних технологій та їх поширення у різних сферах суспільного життя, вони все частіше використовуються як при вчиненні кримінальних правопорушень, так і при їх виявленні (розкритті) та розслідуванні.

Телекомунікаційні послуги надаються суб'єктами господарювання, до числа яких належать:

- *провайдери телекомунікацій* – компанії, що надають телекомунікаційні послуги без права на технічне обслуговування та експлуатацію телекомунікаційних мереж та надання в користування каналів електрозв'язку;
- *оператори телекомунікацій* – компанії, що здійснюють технічне обслуговування та експлуатацію телекомунікаційних мереж за відповідною ліцензією.

Через обладнання та програмне забезпечення провайдерів та операторів телекомунікацій проходить значний об'єм інформації, частина якої залишається в пам'яті обладнання для технологічних цілей і є *статичною інформацією,* а інша частина інформації проходить як «наскрізна» і є *динамічною.*

Статична інформація – це відомості, які зберігаються в операторів та провайдерів телекомунікацій у відповідних інформаційних системах і отримані ними в результаті укладення договору із споживачами та надання телекомунікаційних послуг в минулому. Такі відомості накопичуються, змінюються та протягом певного часу знищуються.

Динамічна інформація представляє собою – відомості, які передаються в мережі, однак не фіксуються, та

не зберігаються в пам'яті телекомунікаційного обладнання без наявності на те потреби, наприклад, зміст розмов, переданих особою даних тощо.

Інформація про споживача та про телекомунікаційні послуги, що були надані споживачеві, може надаватись правоохоронним органам у випадках, визначених законом. Так, доступ до *статичної інформації* можливий на підставі ухвали слідчого судді місцевого суду в порядку тимчасового доступу до речей і документів (глава 15 КПК України), а до *динамічної інформації* на підставі ухвали слідчого судді апеляційного суду в рамках проведення відповідних НС(Р)Д (глава 21 КПК України). В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача (ч.3 ст. 34 Закону «Про телекомунікації»).

Проведене дослідження засвідчує, що найчастіше під час розслідування кримінальних правопорушень працівники правоохоронних органів отримують від операторів та провайдерів телекомунікацій, які надають послуги зв'язку і передачі даних таку інформацію:

1) *відомості щодо наданих телекомунікаційних послуг* (факт надання та отримання послуг, їх вид, тривалість, зміст, маршрути передавання). Встановлене у операторів мобільного зв'язку обладнання та програмне забезпечення фіксує такі відомості:

- номер конкретного абонента (номер SIM, USIM або R-UIM-картки, унікальний ідентифікатор такої картки (IMSI) тощо) та відповідний йому IMEI код мобільного терміналу, яким користувався визначений абонент у мережах операторів стільникового зв'язку України в певний період часу. За наявністю номера абонента, встановлюється IMEI код мобільного терміналу, в якому даний номер використовується (використовувався), а у випадку використання декількох мобільних терміналів з одним і тим же абонентським номером – IMEI коди всіх таких терміналів. За наявністю IMEI коду мобільного терміналу

встановлюється номер абонента (абонентів), який використовував такий термінал мобільного зв'язку у певний період часу;

- вхідні/вихідні дзвінки (дату, час та тривалість з'єднань), SMS та MMS-повідомлення конкретного абонента, що дозволяє здійснити їх вибірку щодо конкретного періоду часу, встановити номери абонентів з якими контактувала визначена особа та IMEI коди їх мобільних терміналів;

- місця перебування конкретного абонента (мобільного терміналу) в момент кожного з'єднання (наприклад, вхідного та вихідного дзвінка, смс-повідомлення, виходу в мережу Інтернет) у межах розташування базових станцій з прив'язкою до часу, категорії самих станцій, порядку естафетної передачі даних, режиму роумінгу тощо. Технічні можливості обладнання операторів мобільного зв'язку дозволяють також визначити, де знаходився абонент в момент розмови (в автомобілі, на вулиці або в будівлі);

- номери ваучерів поповнення балансу конкретного абонента, що дозволяє встановити місце їх придбання;

- переміщення коштів з балансу одного абонента на баланс іншого, або з балансу абонента на банківську картку (у випадку користування послугами ПрАТ «Київстар»).

Крім цього, обладнання телекомунікаційних компаній дозволяє:

- зафіксувати інформацію про з'єднання невизначеного кола абонентських номерів із зазначенням IMEI терміналу (абонентів, що дзвонили з місця події та прилеглої до нього території), що відбулись у межах дії певної базової станції або її соти (параметри дії LAC-SID) за певний період часу, що цікавить (моніторинг);

- визначити адреси розташування та номери базових станцій, які забезпечували зв'язок кінцевого обладнання з визначеними абонентськими номерами;

- здійснити вибірку всіх активних терміналів, які знаходилися в певному квадраті місцевості (місці де було скоєно злочин) у певний час;

- встановити номер абонента користувача Інтернету за допомогою мобільного терміналу за протоколом GPRS/EDGE/CDMA/UMTS, у разі якщо відома його IP адреса і час виходу в Інтернет під нею; GPRS-трафік тощо.

За допомогою одержаних від оператора мобільного зв'язку відомостей стосовно наданих телекомунікаційних послуг можливо:

- встановити місцезнаходження конкретної особи (телефону з абонентським номером) в певний час;

- отримати відомості про засоби зв'язку, використані особою, що цікавить слідство;

- постановити на облік певний номер абонента або IMEI код (номер) мобільного терміналу з подальшим повідомленням замовника в разі появи вказаного абонента або терміналу в мережі (таймер відсутності);

- провести аналіз інформації з огляду перебування володільця кінцевого обладнання в конкретному місці в певний час, наявності комунікацій певного абонента з іншими особами, характер взаємин між ними, їх дати, періодичності, тривалості, тощо;

- виявити коло осіб активного спілкування, в тому числі можливих співучасників злочинних дій (в процесі аналізу протоколів з'єднань абонентських номерів, що використовувались);

- «надати характеристику та індекс закритих груп користувачів»[23];

[23] Вознюк А.А., Алексеєва-Процюк Д.О. Використання ОВС можливостей операторів мобільного зв'язку під час розкриття та розслідування злочинів. *Криміналістика XXI століття:* матер. міжнар. наук.-практ. конф., 25-26 листоп. 2010 р. Харків: Право, 2010. С. 107; Ступаков О.С. Використання можливостей операторів мобільного зв'язку, виробників мобільних операційних систем під час розкриття та розслідування кримінальних правопорушень. *Вісник Академії адвокатури України.* 2013. № 3(28). С. 89-90; Тагієв С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово національної школи суддів України.* 2013. № 2(3). – С. 18.

- встановити анонімні джерела інформації про злочин, визначити коло свідків події злочину;
- спланувати та якісно провести необхідні процесуальні дії. Наприклад, при необхідності затримання особи злочинця, коли його місцезнаходження не встановлено, вищевказана інформація допомагає оптимально обрати місце і час затримання. Затриманню особи в конкретному місці сприяють дані оператора мобільного зв'язку, що надає приблизне місце знаходження працюючого мобільного терміналу за даними базової станції. Такі відомості можна отримати в процесі вивчення деталізації телефонних з'єднань. Крім цього, отримана від оператора мобільного зв'язку інформація в ході допиту може допомогти з'ясувати у допитуваного, з ким саме він розмовляв у певний час, кому належить той чи інший номер телефону, де знаходиться конкретна особа тощо;
- організувати та провести НС(Р)Д з використанням транспортних телекомунікаційних мереж, зокрема, установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), зняття інформації з електронних інформаційних систем (ст. 264 КПК України), під час проведення яких отримати аудіо-, фото-, відеоінформацію (в тому числі із зображенням злочинця і його співучасників;

2) Відомості про споживача, отримані при укладанні договору. Якщо договір укладено із публічним акціонерним товариством «Укртелеком» або іншим оператором стільникового зв'язку на контрактній основі, їх представниками фіксують такі відомості (включаючи персональні):

а) про фізичних осіб (фізичних осіб – приватних підприємців):

- П.І.Б., серія, №, ким виданий документ, що посвідчує особу;

- П.І.Б., свідоцтво про реєстрацію та/або виписка або витяг з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців;
- перелік замовлених абонентом послуг;
- тип кінцевого обладнання (телефонний апарат, факс, модем і т.д.);
- спосіб підключення кінцевого обладнання (індивідуальний, спарений, паралельний, вечірній, односторонньої дії);
- категорія користування (індивідуальний чи колективний);
- адреса встановлення кінцевого обладнання;
- поштова адреса (адреса, за якою надсилати рахунки, листи тощо);

б) про юридичних осіб:

- повне найменування, посада та П.І.Б. керівника чи уповноваженої особи, документ, на підставі якого ця особа діє);
- перелік замовлених Послуг та засобів зв'язку, виділених Абоненту;
- належність до міністерств, відомств та ін.;
- наявність бюджетного фінансування (на підставі довідки фінансового органу про повне фінансування за рахунок бюджетних коштів);
- види діяльності, що дають право на державну підтримку при визначенні вартості Послуг;
- юридична адреса (місцезнаходження);
- поштова адреса (адреса, за якою надсилати рахунки, листи тощо).

Відповідно до п. 7, 8 ч. 1 ст. 162 КПК України, інформація про абонентів та зв'язок належить до охоронюваної законом таємниці. У ч. 2 ст. 5 Закону України «Про захист персональних даних» закріплено, що персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом.

Оператори та провайдери телекомунікацій зобов'язані забезпечувати і нести відповідальність за збереження відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. Тані дані можуть становити інтерес, як для працівників підрозділів карного розшуку, так і органів досудового розслідування.

Безумовно важливим є те, що відомості, отримані від операторів мобільного зв'язку (провайдерів), можуть бути використанні співробітниками правоохоронних органів для встановлення:

1) факту вчинення кримінального правопорушення;

2) часу, місця, способу вчинення кримінального правопорушення;

3) осіб, що скоїли кримінальне правопорушення (у тому числі співучасників та причетних осіб);

4) місцезнаходження знарядь та засобів, що використовувалися під час вчинення злочину, цінного майна тощо.

РОЗДІЛ 5
ЗВЕРНЕННЯ ДО ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ ЩОДО НАДАННЯ ІНФОРМАЦІЇ ПРО КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ І ВЛАСНИКІВ ПОШТОВИХ СКРИНЬОК

В ситуаціях, коли встановлено факт вчинення злочину (наприклад, незаконного збуту наркотичних засобів, зброї, шахрайства тощо) за допомогою мережі Інтернет, співробітники карного розшуку проводять заходи, спрямовані на встановлення IP-адреси користувача, причетного до вчинення протиправних дій, а у подальшому – заходи щодо ідентифікації особи такого користувача й встановлення місцезнаходження відповідного комп'ютерного обладнання та засобів комунікації, їх вилучення й дослідження.

Для встановлення IP-адреси Інтернет-ресурсу (порталу, сайту, веб-сторінки), який містить заборонений контент (пропозиції придбати наркотичні засоби, зброю, інші заборонені до вільного обігу предмети), рекомендується використовувати спеціальні програми, утиліти й команди (наприклад, ping, Trace, Figner LookUp тощо).

Наприклад, необхідно встановити IP-адресу сайту http://rcmarket.us, який є інтернет магазином з продажу наркотиків в Україні та місцезнаходження Інтернет-провайдера, який надає послуги хостингу для цього сайту. З метою встановлення IP-адреси сайту http://rcmarket.us заходимо в меню операційної системи Windows, натискаємо кнопку «Пуск», обираємо пункт меню «Стандартні програми» та «Виконати». У вікні «Запуск програми» набираємо таку команду : ping rcmarket.us, натискаємо кнопку «ОК». За результатами виконання програми отримуємо інформацію про IP-адресу сайту http://rcmarket.us – 64.210.140.214.

Встановивши IP-адресу сайту http://rcmarket.us, наступною дією має бути встановлення компанії Інтернет-провайдера, яка надає послуги хостингу для цього сайту та, відповідно, володіє інформацією про місце перебування користувача. Для цього слід скористатися одним із зазначених сервісів: Whois, 2ip.ru, 2ip.ua, cy-pr.com або інших.

За допомогою сервісу, розміщеного на сайті 2ip.ru та 2ip.ua, встановлено, що сервер, який обслуговує сайт http://rcmarket.us знаходиться у Франції, хостинг провайдером є ONLINE S.A.S. Вказана обставина значно ускладнює роботу правоохоронних органів України, адже потребує взаємодії з правоохоронними органами іншої держави в рамках міжнародної-правової допомоги. Для спрямування запитів закордонним хостинг-провайдерам слід використовувати можливості Департаменту міжнародного поліцейського співробітництва Національної поліції України.

Відомості про осіб, які здійснюють адміністративний та технічний супровід доменного імені (назва посади, прізвище, ім'я, по батькові, номер службового телефону та адреса електронної пошти), є відкритими. Адреса електронної пошти, яка використовується у контактних даних осіб, містить офіційне доменне ім'я реєстратора.

Програмно-технічні засоби, на яких розміщуються державні електронні інформаційні ресурси, для яких здійснюється реєстрація доменного імені повинні розташовуватися на території України.

В ситуації, коли певний Інтернет ресурс має український домен та обслуговується українською хостинг компанією, наприклад, «HostPro», після встановлення провайдера, слідчий звертається до суду для отримання ухвали слідчого судді на тимчасовий доступ до речей і документів (комп'ютерних систем) на адресу встановленого Інтернет-провайдера, хостинг-провайдера та регістратора доменів, у яких:

а) зареєстровано доменне ім'я сайту та які надають послуги розміщення веб-сайту, з якого здійснюється незаконний збут наркотичних засобів, зброї та інших предметів на своїх технічних майданчиках (надають послуги хостингу). Метою направлення ухвали є отримання інформації, що має відношення до кримінального провадження, зокрема:

– коли та протягом якого часу був створений конкретний обліковий запис протиправного характеру;

– з якої IP-адреси було зареєстровано обліковий запис користувача, який створив Інтернет-ресурс із незаконного продажу наркотичних засобів, зброї та інших предметів;

– на кого зареєстрований обліковий запис (повні анкетні дані власників сайту, інформація з панелі адміністрування, IP-адреси, номери телефонів тощо);

– деталізація всіх IP-адрес та часу виходу в даний обліковий запис користувача;

– як здійснювався перегляд даного облікового запису та його наповнення (IP-адреса, установчі дані та час входу);

– яким чином оплачуються послуги за зазначене доменне ім'я (вид платіжної системи, яка використовувалась при поповненні балансу облікового запису користувача даної системи (гаманці, ідентифікатори, види оплат), банківські установи, рахунки тощо;

б) зареєстровано IP-адресу чи поштову скриньку правопорушника – користувача мережі Інтернет, який здійснював електронне листування в реальному часі з невстановленого комп'ютерного обладнання:

– якими є реквізити абонента, який здійснював доступ до мережі Інтернет під певною IP-адресою у певний час доби;

– які IP-адреси використовувалися для створення певного облікового запису;

– які IP-адреси використовуються для з'єднання з цим обліковим записом;

– якими є реєстраційні дані (logs) та абонентська інформація про користувача певного облікового запису (електронної поштової адреси) (наприклад, vkaif@meta.ua);

– якими є відомості про певний обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання;

– яким є зміст адресної книги електронної поштової скриньки;

– яким є зміст усіх вхідних і вихідних повідомлень.

в) є права на адміністрування Інтернет-форумом або чатом, через який здійснювалося протиправне спілкування (з метою встановлення IP-адреси правопорушника)[1]*:*

– час реєстрації даної поштової скриньки і IP-адреси, якими користувався правопорушник;

– установчі дані користувача поштової скриньки;

– через який телефонний номер здійснювалась активація облікового запису;

– якими є деталі всіх сеансів входу до даного облікового запису із зазначенням IP-адрес та часу.

З метою отримання даних переписки (спілкування) в Інтернет-форумі або чаті, яку здійснював розповсюджувач наркотичних засобів, зброї з їх покупцем, доцільно затребувати історію повідомлень певного користувача під певним ніком (мережевим ім'ям).

Якщо з'єднання комп'ютера з мережею Інтернет відбувається через провідний *модем*, слідчий (за відповідним дорученням оперуповноважений карного розшуку)

[1] Кваліфікація та розслідування злочинів, пов'язаних із незаконним збутом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет: метод. рекомендації / О.Ю. Татаров, О.М. Стрильців, В.Б. Школьний та ін. Київ: ГСУ МВС України, Нац. акад. внутр. справ. 2012. С. 13-14.

має затребувати інформацію в Інтернет-провайдера про номер стаціонарного телефону, через який підтримувався зв'язок користувача з провайдером. У подальшому слідчий за визначеним телефонним номером вживає заходів щодо тимчасового доступу до місць, де встановлено модем і підключеного до нього комп'ютерного обладнання та засобів комунікації, а також відпрацьовує їхніх користувачів на причетність до збуту наркотичних засобів, зброї.

Якщо з'єднання з Інтернетом відбувається через підключення за допомогою звичайних *мережевих карт* (LAN) та мережевого кабелю, то слідчий витребує в Інтернет-провайдера інформацію про адресу встановлення комп'ютерної техніки та засобів комунікації, а також особу, яка заключила абонентський договір з провайдером. У подальшому слідчий вживає необхідних заходів щодо тимчасового доступу до комп'ютерної техніки чи засобів комунікацій за визначеною адресою, а також відпрацьовує її користувачів на причетність до збуту наркотичних засобів, зброї.

Якщо електронну поштову адресу створено навмисно для вчинення протиправних дій, правопорушник може користуватися нею з робочих місць у комп'ютерних Інтернет-клубах, кафе, орендованих квартирах, готелях тощо. В цьому випадку необхідно встановити наступне:

– конкретний комп'ютер у внутрішній локальній мережі Інтернет-клубу, кафе або іншого місця, де правопорушник анонімно здійснював свою протиправну діяльність;

– який адміністратор, офіціанти та інші працівники закладу були на зміні під час користування правопорушником мережею Інтернет;

– осіб з числа інших клієнтів, які в той час перебували поблизу комп'ютера правопорушника;

– інший обслуговуючий персонал Інтернет-клубу, кафе, готелю тощо, який міг запам'ятати правопорушника (охоронець, бармен, офіціант, прибиральниця та ін.).

Встановлених осіб необхідно опитати чи встановити особистісні дані (або скласти фоторобот) правопорушника.

Особливу увагу слід звертати на наявність камер відеоспостереження, які б могли зафіксувати правопорушника під час перебування у певному приміщенні, звідки він здійснював вихід у мережу Інтернет. У подальшому здійснюють тимчасовий доступ і перегляд відеоматеріалів, отриманих камерами стеження у місцях появи правопорушника.

Здійснення аналізу отриманих відеоматеріалів дозволить встановити певні ознаки правопорушника (стать, вік, зовнішній вигляд, одяг, інші індивідуальні ознаки тощо), встановити транспортний засіб, яким він користується, а також інших осіб, які володіють відомостями про особу правопорушника (оскільки вони були свідками чи спільниками його протиправних дій, або бачили марку чи реєстраційні номери транспортного засобу, який його підвозив, тощо)[1].

[1] Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рекомендації / О.Ф. Вакуленко, О.М. Стрільців, О.С. Тарасенко та ін. Київ, 2016. С. 36-40.

РОЗДІЛ 6
ТИМЧАСОВИЙ ДОСТУП ДО ІНФОРМАЦІЇ ПРО АБОНЕНТА ТА НАДАНІ ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ, ЯКА ЗНАХОДИТЬСЯ В ОПЕРАТОРІВ ТА ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ

Законодавець передбачив процесуальну можливість тимчасового доступу до інформації, яка знаходиться у операторів та провайдерів телекомунікацій, про зв'язок абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання (п.7 ст. 162, п 6. ст. 163 КПК України) як захід забезпечення кримінального провадження. Ця інформація міститься в речах і документах та віднесена до охоронюваної законом таємниці*, тимчасовий доступ до яких може бути надано слідчим суддею місцевого суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування за відповідним клопотанням (глава 15 КПК України).

Однак у слідчій практиці трапляються випадки, коли слідчі у клопотанні, фактично, ставлять питання про надання дозволу на втручання у приватне спілкування*, тобто проведення негласної слідчої (розшукової) дії, що є

---

* Відповідно до ст. 162 КПК України до охоронюваної законом таємниці, яка міститься в речах і документах, належать: … відомості, які можуть становити банківську таємницю; особисте листування особи та інші записи особистого характеру; інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних.

* Втручання у приватне спілкування здійснюється в рамках негласних слідчих (розшукових) дій. Різновидами втручання в приватне спілкування є: 1) аудіо-, відеоконтроль особи; 2) арешт, огляд і виїмка кореспонденції; 3) зняття інформації з транспортних телекомунікаційних мереж; 4) зняття інформації з електронних інформаційних систем, які проводяться виключно на підставі ухвали слідчого судді (ч.1 ст. 258 КПК України).

предметом розгляду слідчих суддів апеляційного суду. *Так, слідчий суддя Дарницького районного суду м. Києва, розглянувши клопотання старшого слідчого СВ ФР ДПІ у Дарницькому районі ГУ Міндоходів у м. Києві про надання дозволу на проведення виїмки документів, які перебувають у володінні ТОВ «Воля-Кабель», а також надання доступу до інформації про абонента, який використовував зазначений у клопотанні IP-адрес, відмовив у задоволенні клопотання. В ухвалі від 12.03.2014 року суддя з посиланням ст.264 КПК України зазначив, що отримати доступ до вказаної інформації, що міститься в електронній інформаційній системі, можливо лише під час проведення негласних слідчих (розшукових) дій, дозвіл на проведення яких дається головою чи за його визначенням іншим суддею суду апеляційної інстанції (Справа № 753/4424/14-к).*

Згідно з ч.4 ст.258 КПК України втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Відповідно до ст.9 Закону України «Про телекомунікації» охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України.

Алгоритм доступу до речей і документів, які містять охоронювану законом таємницю, регламентований ст. 165 КПК України. У ній зазначається, що цей доступ здійснюється шляхом виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів.

Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

Тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення (ст. 159 КПК України).

Відповідно до ст. 160 КПК України сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий доступ до речей і документів, за винятком зазначених у статті 161 цього Кодексу (листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, що представляє клієнта у зв'язку з наданням правової допомоги, та додані до них об'єкти). Слідчий має право звернутися із зазначеним клопотанням за умови погодження прокурором. Отже, законодавець визначив вичерпний перелік осіб, які мають право звертатися з відповідним клопотанням (слідчий або прокурор), і недотримання вказаної вимоги закону є підставою для відмови в задоволенні клопотання.

Слідчий суддя не повинен брати до провадження клопотання слідчого, якщо воно не було погоджено прокурором, або той із ним не погодився, або з клопотання незрозуміло, який саме прокурор дав згоду.

Тимчасовий доступ до речей і документів не допускається, якщо слідчий, прокурор у клопотанні не доведе, що:

1) існує обґрунтована підозра щодо вчинення кримінального правопорушення такого ступеня тяжкості, що може бути підставою для застосування заходів забезпечення кримінального провадження;

2) потреби досудового розслідування виправдовують такий ступінь втручання у права і свободи особи, про який ідеться в клопотанні слідчого, прокурора;

3) може бути виконане завдання, для виконання якого слідчий, прокурор звертається із клопотанням (ч.3 ст. 132 КПК України).

Фактичною підставою для отримання інформації про з'єднання мобільних терміналів є наявність відомостей про те, що:

- підготовка, учинення або приховування злочину здійснювалися з використанням мобільного терміналу;

- особа, місцезнаходження якої встановлюється, користувалася (користується) мобільним терміналом;

- предметом злочинного посягання є мобільний термінал.

Правовими підставами отримання інформації про абонента та зв'язок є наявність достатніх підстав вважати, що ці відомості:

- перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи (оператора чи провайдера телекомунікацій);

- самі по собі або в сукупності з іншими відомостями, речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні (ч. 5 ст. 163 КПК)[26].

Частиною 2 статті 160 КПК України встановлено вимоги до клопотання про тимчасовий доступ до речей і документів. *У клопотанні про тимчасовий доступ до речей і документів обов'язково мають бути вказані такі відомості:*

- короткий виклад обставин кримінального правопорушення, у зв'язку з яким воно подається;

[26] Використання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, їх транспортних телекомунікаційних мережах, під час розслідування злочинів: метод. рекомендації / С.С. Чернявський, О.Ю. Татаров, Д.О. Алексєєва-Процюк та ін. Київ: Нац. акад. внутр. справ, 2013. С. 15-16.

- правова кваліфікація кримінального правопорушення із обов'язковим зазначенням статті Кримінального кодексу України;
- повні і конкретні відомості про речі і документи, тимчасовий доступ до яких планується отримати;
- підстави вважати, що речі і документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи. За відсутності конкретних даних у клопотанні щодо фізичних або юридичних осіб, які мають надати тимчасовий доступ до речей і документів, а так само недоведеності підстав вважати, що речі і документи перебувають у певних осіб, слідчі судді відмовляють у їх задоволенні;
- суттєве значення речей і документів (наприклад, документи самі по собі, а також в сукупності з іншими речами і документами кримінального провадження мають суттєве значення для встановлення важливих обставин у кримінальному провадженні) для встановлення події кримінального правопорушення; винуватості обвинуваченого у вчиненні кримінального правопорушення, форми вини, мотиву, мети вчинення кримінального правопорушення та інших обставин у кримінальному провадженні;
- обґрунтування необхідності вилучення речей і документів, якщо відповідне питання порушується стороною кримінального провадження. Відповідно до ч.7 ст.163 КПК України слідчий суддя, суд в ухвалі про надання тимчасового доступу до речей і документів може дати розпорядження про надання можливості вилучення речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що без такого вилучення існує реальна загроза зміни або знищення речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів. Як правило такі факти мають місце в ситуаціях, пов'язаних із необхідністю вилучення документів,

які знаходяться у володінні банківських установ та стосуються функціонування рахунків, а саме, роздруківок руху коштів, заяв на відкриття рахунку, карток із зразками підписів та відбитка печатки, документів, які б були підставою для ідентифікації особи, уповноваженої діяти від імені власника рахунку тощо.

У разі подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, зазначається про можливість використання як доказів відомостей, що містяться в речах і документах (наприклад, інформація, що міститься в речах і документах має суттєве значення для встановлення осіб, причетних до вчинення кримінального правопорушення, а також те, що зазначена інформація для кримінального провадження буде мати доказове значення і забезпечувати виконання завдань кримінального провадження щодо швидкого, повного та неупередженого розслідування[27]), та обґрунтовується *неможливість іншими способами довести обставини, які передбачається доказати за допомогою цих речей і документів*.

Слушними у даному випадку є положення згаданих вище методичних рекомендацій *«Використання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, їх транспортних телекомунікаційних мережах, під час розслідування злочинів», де* вказується, що при вирішенні цього питання необхідно керуватись *п. 16 Інформаційного листа ВССУЦКС від 29.01.2013 № 223–158/0/4–13 «Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні»*. «Відповідно до вказаного Інформа-

[27] Див.: Ухвала Сєвєродонецького міського суду Луганської області від 25 січня 2017 року по справі № 428/776/17 у провадженні № 1-кс/428/356/2017. URL: https://opendatabot.com/court/64816676-36d072a61dced8f7cd16eb2937c431c9

ційного листа, слідчі судді мають враховувати, що однорідні питання, які потрібно з'ясувати в рамках одного кримінального провадження шляхом застосування одного або різних видів заходів забезпечення, пов'язаних між собою (при цьому необхідність з'ясування таких питань обґрунтовується однаковими обставинами), можуть ініціюватися слідчим (прокурором) *у рамках одного клопотання та вирішуватися слідчим суддею в одній ухвалі.* Такий підхід доцільно застосовувати для розгляду клопотань про надання тимчасового доступу до документів, які знаходяться в операторів і провайдерів телекомунікацій та містять інформацію про абонента та зв'язок (ст. 159, п. 7 ч. 1 ст. 162 КПК).

Так, у разі необхідності отримання інформації у рамках одного кримінального провадження з однаковим обґрунтуванням такої потреби вважають за доцільне об'єднання в межах одного клопотання, які стосуються отримання тимчасового доступу (можливості ознайомитися та зробити копії) до документів, що знаходяться в оператора (провайдера), за умови реальної технічної можливості операторів (провайдерів) телекомунікацій надати таку інформацію, та які містять:

- інформацію про ідентифікаційні ознаки кінцевого обладнання телекомунікацій (абонентський номер SIM-картки, IMEI, MAC-адреса, IP-адреса тощо), яке перебувало у зоні дії певних базових станцій у певний час;
- інформацію про прізвища, імена, по батькові та інші відомості про споживача телекомунікаційних послуг та абонентів зазначеного кінцевого обладнання телекомунікацій (за наявності таких відомостей);
- інформацію про типи з'єднань зазначеного кінцевого обладнання телекомунікацій (вхідні та вихідні з'єднання) за певний період часу включно із зазначенням дати і часу, тривалості таких з'єднань, маршрутів передавання даних (при цьому зазначений період часу може завершуватися після пред'явлення ухвали до виконання,

тобто передбачати надання доступу – можливості постфактум ознайомитися та зробити копії – до інформації щодо з'єднань, які відбудуться у майбутньому);

- зазначену вище інформацію щодо кінцевого обладнання телекомунікацій, з якими з'єднувалося кінцеве обладнання телекомунікацій, що перебувало у зоні дії певних базових станцій у певний час, та щодо їх наступних з'єднань;
- іншу інформацію про телекомунікації».

До клопотання слідчого, прокурора про застосування тимчасового доступу до речей і документів в обов'язковому порядку додається належним чином засвідчена копія витягу з ЄРДР щодо кримінального провадження, в рамках якого подається клопотання.

Кримінальний процесуальний закон не передбачає повноважень суду щодо повернення клопотань про тимчасовий доступ до речей і документів, на відміну від інших заходів забезпечення кримінального провадження, у разі недотримання стороною кримінального провадження вимог закону. Однак у судовій практиці трапляються випадки постановлення слідчими суддями і таких рішень, зокрема з підстав порушення правил територіальної підсудності[28]. У разі невідповідності клопотання про його застосування вимогам ч. 2 ст. 160 КПК слідчий суддя вправі відмовити у його задоволенні, належним чином обґрунтувавши прийняте ним рішення.

Крім цього, у главі 15 КПК України не визначено строк, протягом якого слідчий суддя, суд має розглянути клопотання про тимчасовий доступ до речей і документів. Однак, враховуючи зміст положень ч.6 ст.9 КПК України, правильним є розгляд клопотання не пізніше трьох днів із дня його надходження до суду, а у разі,

[28] Див.: Ухвала Солом'янського районного суду м. Києва від 25 березня 2014 року по справі № 760/6158/14-к. URL: http://www.reyestr.court.gov.ua/Review/49510022

якщо особа, яка подала клопотання, обґрунтує у ньому наявність реальної загрози зміни або знищення речей і документів, слідчий суддя має розглянути клопотання невідкладно.

Також, кримінальний процесуальний закон не містить конкретної вказівки слідчому судді на те, яким чином необхідно діяти в разі неявки на розгляд клопотання про тимчасовий доступ до речей і документів сторони кримінального провадження, якою таке клопотання було подане, з огляду на положення ч.4 ст.163 КПК України, згідно з якою клопотання цієї категорії розглядається за участю сторони кримінального провадження.

В такому випадку слідчим суддям необхідно керуватись ч.5 ст.163 КПК України, відповідно до якої слідчий суддя вправі постановити ухвалу про тимчасовий доступ до речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що мають місце обставини, передбачені п.п.1, 2, 3 ч.5 ст.163 КПК України. Разом з цим, неявка без поважної причини сторони кримінального провадження, якою подано клопотання про тимчасовий доступ до речей і документів, свідчить про фактичне не підтримання клопотання та недоведення вказаних обставин, що може оцінюватись як підстава для відмови в задоволенні такого клопотання[29].

Відтак, під час тимчасового доступу до речей і документів у операторів та провайдерів телекомунікацій, слідчий, прокурор можуть отримати інформацію про:

- зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо;

[29] Тютюн Т.М. Узагальнення проблемних питань, які виникають при розгляді клопотань про тимчасовий доступ до речей і документів. URL: http://www.apcourtkiev.gov.ua/wp-content/uploads/2015/07/12014-kr.pdf

- ідентифікаційні ознаки кінцевого обладнання телекомунікацій (абонентський номер, SIM-карту, IMEI, MAC адреси, IP-адресу та ін.);

- місце перебування у минулому ідентифікованого кінцевого обладнання телекомунікацій (за азимутом) у зоні дії певних базових станцій у певний час або його проміжок;

- прізвища, імена, по-батькові та інші відомості про абонентів телекомунікаційних послуг;

- маршрути переданої інформації незалежно від виду телекомунікаційної мережі;

- вихідне з'єднання – номер сторони, з якою зв'язувалися, навіть якщо зв'язок не було встановлено;

- вхідне з'єднання – номер сторони, яка зв'язувалась, навіть якщо зв'язок не було встановлено;

- початок, кінець та тривалість з'єднання, яке відбулося без розкриття змісту переданої інформації;

- фактичне місце призначення та проміжний абонентський номер у разі, якщо зв'язок був переадресований[30].

[30] Використання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, їх транспортних телекомунікаційних мережах, під час розслідування злочинів: метод. рекомендації / С.С. Чернявський, О.Ю. Татаров, Д.О. Алексєєва-Процюк та ін. Київ: Нац. акад. внутр. справ, 2013. С. 17.

РОЗДІЛ 7
ОТРИМАННЯ ДОСТУПУ ПРАЦІВНИКАМИ КАРНОГО РОЗШУКУ ДО ІНФОРМАЦІЇ, ЯКА СТАНОВИТЬ БАНКІВСЬКУ ТАЄМНИЦЮ

Під час виявлення та розслідування злочинів у працівників карного розшуку може виникнути необхідність отримання відомостей, які становлять банківську таємницю.

Під банківською таємницею розуміють – інформацію щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку.

До банківської таємниці відносять відомості та інформацію: 1) про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2) про операції, проведені на користь чи за дорученням клієнта, та здійснені ним угоди; 3) про фінансово-економічний стан клієнтів; 4) про системи охорони банку та клієнтів; 5) про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; 6) стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) щодо звітності банку, за винятком тієї, що підлягає опублікуванню; 8) про коди банків для захисту інформації; 9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності (ст. 60 ЗУ Про банки і банківську діяльність).

Відповідно до чинного законодавства, Інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:

1) на письмовий запит або з письмового дозволу відповідної юридичної чи фізичної особи;

2) за рішенням суду формою оформлення якого є ухвала суду про розкриття банківської таємниці та тимчасовий доступ до речей та документів. Для отримання такої ухвали слідчий готує та направляє до суду відповідне клопотання, в якому крім обставин кримінального правопорушення, речей та документів, до яких намагається отримати доступ слідчий, також наводить докази та надає документи, які підтверджують обставини, на які він посилається у своєму клопотанні, інакше, суд може прийняти рішення про відмову слідчому у задоволенні клопотання. У клопотанні також повинна бути зазначена особа, яка буде безпосереднім виконавцем ухвали суду про розкриття банківської таємниці та тимчасовий доступ до речей та документів. Під час розгляду клопотання слідчим суддею – слідчий має підтримувати своє клопотання особисто, або направити до суду заяву з проханням розглянути клопотання без його участі. У разі позитивного вирішення питання, слідчий суддя приймає рішення про задоволення клопотання та зобов'язує службових осіб певної фінансової установи розкрити банківську таємницю та надати тимчасовий доступ до речей та документів, що містять банківську таємницю (наприклад, відомості про рух грошових коштів із зазначенням дати виконання платежів з повною розшифровкою призначення платежу та реквізитів контрагентів по рахунку: НОМЕР (українська гривня), за період з 05.01.2017 року по 06.10.2017 року на паперових та оптичних носіях).

За ухвалою суду про розкриття інформації, що становить банківську таємницю, банк розкриває інформацію в обсязі, визначеному рішенням суду. Банк зобов'язаний надати тимчасовий доступ до зазначених в ухвалі слідчого судді, суду речей і документів, які містять інформацію, що становить банківську таємницю, особі, зазначе-

ній в ухвалі. Представник банку в разі проведення вилучення (виїмки) речей і документів, які містять інформацію, що становить банківську таємницю, на підставі ухвали зобов'язаний:

- ознайомитися з оригіналом ухвали, що пред'являється особою, зазначеною в ухвалі;
- отримати від особи, що пред'явила ухвалу:

а) копію ухвали;

б) опис речей і документів, які містять інформацію, що становить банківську таємницю, та вилучаються на виконання ухвали;

в) копію протоколу про вилучення (виїмку) речей і документів, які містять інформацію, що становить банківську таємницю (у разі складення протоколу особою, що пред'явила ухвалу).

Банк зобов'язаний:

- виготовити копії з оригіналів документів, які містять інформацію, що становить банківську таємницю, та вилучаються. Ці копії документів засвідчуються підписом представника банку та залишаються в банку замість вилучених оригіналів;
- здійснити опис майна, яке містить інформацію, що становить банківську таємницю та вилучається, який засвідчується підписом представника банку та залишається в банку;
- зберігати в окремих справах копії ухвал, ухвал слідчого судді, описи документів, майна, що вилучалися на виконання ухвал, копії протоколів про вилучення (виїмку) речей і документів, які містять інформацію, що становить банківську таємницю, обшуку або огляду[31];

[31] Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова правління Національного банку України від 14.07.2006 N 267. URL: http://zakon3.rada.gov.ua/laws/show/z0935-06

3) на письмову вимогу (за письмовим запитом) органів прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро України, Антимонопольного комітету України – стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу (ст. 62 ЗУ Про банки і банківську діяльність)[32]. На фізичних осіб, які не є суб'єктами підприємницької діяльності, дія даного нормативно-правового акту не розповсюджується.

[32] Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III. URL: http://zakon2.rada.gov.ua/laws/show/2121-14

РОЗДІЛ 8
ВИДИ ТА ДЖЕРЕЛА ЦИФРОВИХ ДОКАЗІВ, ТИПОВІ СПОСОБИ ЇХ ПРИХОВУВАННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЇХ ВИЯВЛЕННЯ ТА ДОСЛІДЖЕННЯ

При виявленні злочинів, що вчиняються із використанням сучасних інформаційно-телекомунікаційних технологій увага співробітників оперативних підрозділів має бути спрямована на пошук електронних (цифрових) доказів (слідів).

Цифровий (електронний) доказ – це інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для кримінального провадження. Цифровий доказ має такі особливості: 1) є прихованим; 2) легко перетинає кордони юрисдикції; 3) може бути змінений, пошкоджений або знищений; 4) може бути вразливим – чутливим до часу.

Цифрові докази можуть також містити речові докази, такі як ДНК чи відбитки пальців рук та долонь особи, тому повинні бути збережені для відповідного експертного дослідження. Всі маніпуляції з електронними пристроями, які можуть містити такі сліди, мають проводитись особою, що має відповідну підготовку (освіту) та у латексних рукавичках.

До основних характеристик таких доказів належать:

- неможливість безпосереднього виявлення людиною на фізичному рівні;
- нестійкість;
- зміна або знищення в процесі звичайної експлуатації пристрою;
- копіювання без втрати якості.

Виділяють три основних види таких слідів (доказів):

1) Мережеві цифрові сліди.
2) Локальні цифрові сліди.

3) Електронна інформація.

До мережевих цифрових слідів – відносять відомості, що зберігає оператор (провайдер) телекомунікації, які умовно можна поділити на:

- *дані про користувача* (контактні дані, адреса телефон, ім'я та ін.;
- *дані про сеанси зв'язку* (первинний номер телефону, сеанси зв'язку, LOG-файли реєстрації доступу до тих чи інших інформаційних систем, типи використаних протоколів маршрутизації, статистичні або динамічні IP-адреси тощо).

Локальними цифровими слідами – є сліди, що залишаються на комп'ютерах, які використовуються для вчинення протиправних дій, або через які проходить або надходить інформація (сліди прямого впливу, докази опосередкованого впливу, викривлення інформації, знищення інформації, блокування інформації, відсутність доступу, порушення конфіденційності, порушення роботи комп'ютера тощо).

Електронною інформацією можуть бути: цифрові фото зображення, відео контент; текстові документи; веб-сайти (сторінки); метадані; бази даних.

Джерелами цифрових слідів можуть бути:

1. *Електронна поштова скринька.* Особливу цінність представляє листування осіб та прикріплені файли (документи, фото,- відео файли тощо). Слід також пам'ятати, що кожен відправлений (отриманий) лист супроводжує комплекс додаткової службової інформації, що містить короткі відомості про відправника листа та його електронну адресу (наприклад, Головаш Семен Вікторович gsv90@ukr.net), відомості про одержувача листа (наприклад, Петров Максим petrov-m@i.ua), дату відправлення у форматі (наприклад, четвер, 8 жовтня 2018, час 22:47, часовий пояс +03:00), тему листа (наприклад, «Прайси»), те, що повинно бути передано адресату (або конкретний

текстовий фрагмент тощо). Кожному електронному повідомленню автоматично присвоюється тема (заголовок), яка містить службову інформацію для поштових серверів і програм, через які воно проходить. Обов'язкові поля заголовку електронного листа містять інформацію про поштову програму, дату написання листа, адресу поштового сервера провайдера, а також адресу відправника.

Також слід перевірити наявність інстальованих програм для перегляду отриманих та відправки електронних поштових повідомлень (Microsoft Exchange, Apple Mail, TheBat, Mozilla Thunderbird), які містять вивантажені отримані та надіслані повідомлення; збережені логіни та паролі для електронних поштових скриньок; надіслані файли.

2. *Інтернет-сайти*, які відвідувала особа. Інстальовані програми (веб-браузери для перегляду веб-сайтів Mozilla Firefox, Microsoft Explorer, Microsoft EDGE, Opera, Google Chrome, Apple Safari) у налаштуваннях містять історію пошуку і відвідування певних ресурсів; збережені логіни та паролі для ресурсів із авторизацією; історію завантажених файлів. Подібні відомості доступні й провайдеру, який надає доступ до мережі Інтернет.

3. *Інстальовані програми для обміну миттєвими повідомленнями* (Telegram, Skype, Viber, WhatsApp., Jabber), які містять вивантажені отримані та надіслані повідомлення; збережені логіни та паролі для облікових записів; надіслані файли); а також *програми синхронізації із смартфонами та планшетами* IOS ITunes, які містять резервну копію смартфона або планшета; збережені файли у тому числі фото, відео, логін ICloud тощо.

4. *Профіль особи у соціальних мережах*. Ретельно вивчивши відомості, розміщені конкретною особою в соціальній мережі, можна отримати значиму інформацію: особисту персональну інформацію про особу та її рідних (ПІБ, номер телефону, електронну пошту, місце роботи,

освіту, дату народження і відомості про місцеперебування (минуле чи теперішнє)), соціальні та особисті зв'язки, уподобання (пристрасті). По спільних фотографіях легко встановити контакти особи, у профілях соціальних мереж яких можуть залишитися отримані повідомлення, а по фотознімках на фоні різних об'єктів (наприклад, вікна або балкона), визначити будинок, який був за вікном, виміряти кут та визначити поверх і квартиру, встановивши місцезнаходження.

5. *Рахунок в електронних платіжних системах* (наприклад, «Qiwi-гаманець» та інші). При реєстрації в системі користувач вводить свої дані (додавання документів не потрібно) та власний мобільний номер телефону, на який приходить код підтвердження. Після реєстрації особа може оплачувати різні товари та послуги, зберігати грошові кошти, а також здійснювати різні обмінні операції (наприклад, переказ грошей на пластикову карту або перекази через обмінні системи) тощо. Відомості про всі проведені операції залишаються в пам'яті системи та за необхідності можуть бути витребувані правоохоронними органами.

6. *Локальна мережа.* Це найпростіша форма мережі, що сполучає в одну групу комп'ютери або зв'язує їх з потужнішим ПК (наприклад, з мережевим сервером). Отримавши доступ до такої мережі, правоохоронці матимуть можливість доступу до ресурсів (папок, програм, файлів, тощо) всіх з'єднаних між собою комп'ютерів. За наявності локальної мережі, доказова інформація про протиправну діяльність може бути виявлена як в сервері так і робочих комп'ютерах мережі.

7. *Мережеві пристрої (роутери, маршрутизатори тощо).* При виявленні мережевих роутерів, маршрутизаторів перш за все слід встановити, чи під'єднані до нього персональні комп'ютери, смартфони, планшети, інші електронно-обчислювальні засоби або мобільні термінали.

Дізнатися про це можливо при перегляді локальної адреси роутера, логін та пароль якого за замовчуванням, зазвичай вказані на зворотній стороні мережевого пристрою. Далі, при відвідуванні локальної адреси роутера за допомогою веб-браузера будь-якого пристрою під'єднаного до роутера буде демонструватися зовнішня адреса роутера, а також кількість під'єднаних до нього пристроїв, а також їх мак-адреси, Ір-адреси, мережеві імена.

8. *Комп'ютерна система* (персональний комп'ютер, ноутбук), що складається з апаратного та програмного забезпечення (плати, мікропроцесора, жорсткого диску, пристроїв пам'яті тощо), які обробляють та зберігають дані. При дослідженні вмісту жорсткого диску можуть бути виявлені: встановлене та використане програмне забезпечення, документи, фотографії, повідомлення електронної пошти прикріплені файли до них, бази даних, інформація про фінансові операції, історія відвіданих Інтернет сторінок, файли журналів подій, LOG-чатів, використані пристрої, будь-яка ідентифікаційна інформація, пов'язана з комп'ютерною системою; інформація про з'єднання, у тому числі Інтернет-протоколу (IP) та адреси локальної мережі (LAN), пов'язані з комп'ютерами і пристроями; настройки трансляцій; адреси карти доступу до середовища (MAC), або мережевої карти (NIC). Отримана у такий спосіб інформація може підтверджувати факт підготовки або вчинення певних протиправних дій (передавання погроз, проведення перемовин при замовленні злочину, спілкування злочинців при плануванні чи вчиненні правопорушення тощо) та факт вчинення злочину (цифрові фотографії, відео- звукозаписи механізму злочину в цілому або його частини тощо).

9. *Пристрої зберігання даних.* До найпоширеніших носіїв цифрової інформації належать: *зовнішні жорсткі диски* (3.5 та 2.5. жорсткі диски; мережеві запам'ятовувальні пристрої); *флеш-накопичувачі* (накопичувачі з інтерфейсами підключення USB 2.0, USB 3.0, USB Type C

тощо); *змінні носії* (дискети; Zip диски; компакт-диски); *карти пам'яті* (Smart Media (SM) карта; Secure Digital (SD); *периферійні пристрої* (клавіатура і миша; мікрофони; USB хаби і FireWire; веб-камери; читачі карти пам'яті; VoIP пристрої); *інші пристрої* (стрічкові накопичувачі даних; обладнання для спостереження; цифрові фотоапарати; відеокамери; цифрові аудіорекордери; цифрові відеореєстратори; MP3-плеєри; супутникові аудіо, відео ресивери, карти доступу; відеоігрові приставки; гарнітура комп'ютерного чату; SIM-карт-рідер; приймач (GPS); зчитувач відбитків пальців).

10. *Мобільні термінали зв'язку* (мобільні телефони, смартфони). З мобільного терміналу може бути вилучено: ідентифікаційні данні про апарат (модель, IMEI); телефонну книгу; SMS-повідомлення; календар; нотатки; фотозображення; відео- та звукозаписи; збережену інформацію у веб-браузерах; документи різних форматів; архіви програм обміну повідомленнями (месенджерів Viber, WhatsApp тощо); програми-клієнти соціальних мереж (ВКонтакте, Facebook, Twitter тощо); програми-клієнти сервісів електронної пошти. Отримана інформація може мати безпосереднє відношення до вчинення злочинів (містить зображення потерпілих, відомості про механізм злочину, місця приховання слідів, звукозаписи перемовин, інформацію про з'єднання між абонентами тощо) або використана при складанні психологічного портрету особи, або в якості бази для встановлення психологічного контакту.

11. *Записи з камер систем відеоспостереження*. Сучасні камери відеоспостереження фіксують обстановку та обставини події, осіб, причетних до злочину, транспортні засоби. За умови їх правильного процесуального отримання (в рамках тимчасового доступу до речей і документів), вони можуть бути використані у кримінальному провадженні в якості доказу (електронного документу).

З метою приховування віртуальних доказів (слідів) злочинці застосовують:

Анонімайзери – засоби приховування даних в мережі з метою запобігання ідентифікації джерела трафіку і місця призначення завдяки використанню анонімних мереж, анонімних проксі серверів, анонімних Веб-проксі);

VPN (Virtual Private Network) – технологія, яка забезпечує зашифроване з'єднання поверх інтернет-з'єднання, що використовується.

Tor – веб-браузер із вбудованим анонімайзером TCP / IP-трафіку і проксі-фільтром вмісту веб-сторінок для анонімної роботи в мережі Інтернет.

DarkNet (з англ. – «прихована мережа», також – Dark Web) – прихована мережа Інтернет-з'єднань, що існує на базі звичайного інтернету, але використовує виключно захищені проксі-сервера та інтернет-з'єднання, які унеможливлюють відстеження користувачів і сайтів.

I2P – мережа всередині мережі, анонімна оверлейна мережа, створена для захисту даних, що передаються від зовнішнього спостереження і нагляду провайдером.

RetroShare – анонімна криптографічна платформа, що забезпечує безсерверний обмін листами, миттєвими повідомленнями і файлами за допомогою шифровано мережі.

Freenet – однорангова мережа, призначена для децентралізованого розподіленого зберігання даних без можливості їх критики, з метою надати користувачам свободу слова в Інтернеті шляхом забезпечення їх суворої анонімності в мережі.

До основних методів виявлення незаконних дій в мережі Інтернет належать:

1. *Перехоплення и дослідження трафіку*. На основі аналізу вмісту мережевого трафіку є можливість визначити й довести факт вчинення користувачем певних дій у мережі, а також отримати інформацію про будову програм, інформаційних систем і мереж.

2. *Дослідження статистики трафіку*. Це дозволяє проводити накопичення, обробку, класифікацію, контроль і модифікацію мережевих пакетів в залежності від їх вмісту в реальному часі.

3. *Дослідження LOG-файлів веб-сервера.* LOG – це журнал автоматичної реєстрації подій, які фіксуються в рамках будь-якої програми. (Log file) фіксує інформацію про події в хронологічному порядку (час з'єднання, MAC-адресу мережевого пристрою, тривалість сеансу, надану IP-адресу, та інші дані), що сприятиму встановленню місця з'єднання, мережевого обладнання та особи, що вчинила незаконні дії.

4. *Дослідження системних LOG-файлів.* Створення LOG-файлів подій в операційній системі підвищує ймовірність виявлення злочинця, подальшого встановлення його місцезнаходження і викриття. Також цей процес сприяє виявленню вразливостей захищається системи.

5. *Дослідження LOG-файлів поштового сервера і заголовків електронної пошти.* LOG-файли розміщуються в каталозі / var / log / exim /.

Розглянемо приклад фрагменту *LOG*-файлу з розшифровкою:

2004–04–13 07:38:59 1BDElF-0006fT-Jz@post.** H=(interost.ru) [82.148.19.253] P=esmtp S=41294

2004–04–13 07:38:59 1BDElF-0006fT-Jz => *** R=localuser T=local_delivery

2004–04–13 07:38:59 1BDElF-0006fT-Jz Completed

Перший рядок каталогу містить – запис про прийняття повідомлення, де першими йдуть дата і час повідомлення, далі внутрішній ідентифікатор повідомлення, далі знак операції (прийом, доставка тощо), далі адреса відправника (аргумент, команди, IP-адреса з якого прийнято повідомлення , протокол), розмір повідомлення в байтах, користувач, від імені якого запускалася команда, власний ідентифікатор повідомлення.

Другий рядок свідчить про те, що повідомлення практично відразу було доставлено в локальний поштовий ящик***, за відповідною адресою ****@post.**.

Третій рядок зазначає дату і час завершення обробки листа.

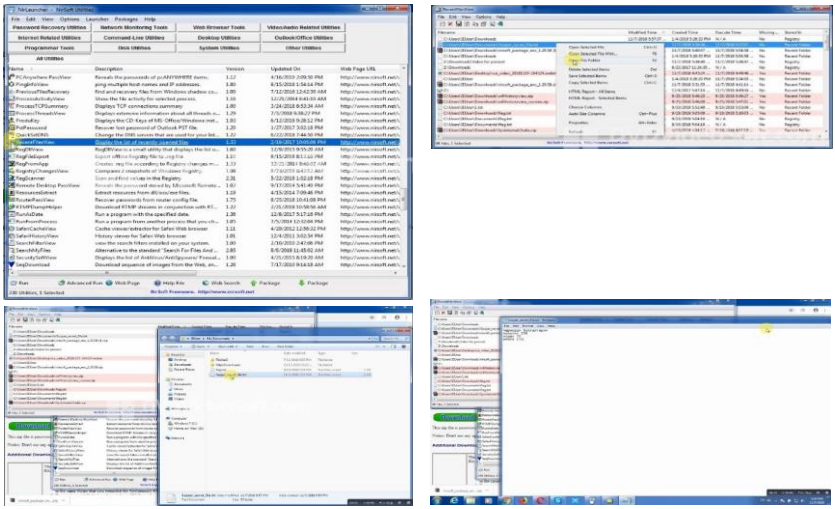
6. *Встановлення належності і знаходження IP-адреси.* Після встановлення IP-адреси з якої за допомогою комп'ютерної техніки було вчинено злочин, постає завдання встановити особу, яка використовувала цю техніку і місце її знаходження, що відповідає наступній схемі:

«(Злочин) – (IP-адреса) – (комп'ютер) – (злочинець)».

За допомогою спеціальних технічних засобів (програмного забезпечення) фіксується IP-адреса, з якої здійснювалася протиправна діяльність. Далі встановлюється провайдер, який допомагає визначити адресу підключення до мережі Інтернет, яка відповідає встановленій IP-адресі та персональний комп'ютер, який працював з цієї IP-адреси. Після цього доводиться факт використання комп'ютером у певний час підозрюваним.

Для роботи з цифровими доказами (слідами) можуть застосовувати наступні науково-технічні засоби та програмне забезпечення:

NirLauncher – безкоштовний багатофункціональний пакет портативних утиліт для обслуговування ОС Windows, який містить інструменти для налаштування і оптимізації операційної системи, управління прихованими параметрами Windows і відкриття доступу до зашифрованих даних встановлених програм. За її допомогою отримується доступ до: параметрів операційної системи, інформації щодо останніх відкритих файлів, зовнішніх юсб-пристроїв, історії відвідування веб-сторінок, пошукових запитів, збережених паролів браузера тощо. Також за її допомогою здійснюється перевірка незмінності отриманих цифрових даних.



NetAnalysis – програмне забезпечення, що забезпечує можливість вилучення існуючої і відновлення видаленої інформації з персонального комп'ютера, її подальшого аналізу та представлення у зрозумілому форматі. До основних можливостей цієї програми належать: *відновлення та аналіз інформації*, що залишається після використання веб-браузерів; *перегляд кеш-файлів* в режимі Offline (автоматичне переведення HTML сторінок з кешу, корегуючи графіку, як на звичайній веб сторінці, перегляд прямо з кешу JPEG та інші фотографії, які були переглянуті підозрюваним); *авторозподіл веб-сайтів* користувача відповідно до його пошукових запитів; *відновлення видалених даних* (історії використання веб-браузерів тощо).

Defacto – Программа, що призначена для експрес-інвентаризації програмного забезпечення, фактично встановленого на жорсткому диску персонального комп'ютера.

Апаратні та програмні засоби для дослідження мобільних пристроїв:

Cellebrite UFED Touch 2 – портативний апаратно-програмний комплекс для зняття і дослідження даних з мобільних пристроїв. Забезпечує повний доступ до даних на фізичному, логічному і на рівні файлової системи. Дозволяє аналізувати, формувати в звіт отриману інформацію.

За допомогою UFED Touch 2 можна отримати наступні готові дані: інформацію про пристрій; бездротові мережі; журнал викликів; журнал перегляду веб сторінок; записи календаря; контакти; місце розташування пристрою; паролі; історію пошуків; сповіщення пристрою; список додатків; пристрої Bluetooth; облікові записи користувача; файли Cookie; чати; електронну пошту.

XAMN Horizon – комплект аналітичного програмного забезпечення, розроблений для зіставлення даних, вилучених зі смартфонів, планшетів та інших мобільних пристроїв за допомогою експертних інструментів;

Програми пошуку і виявлення віртуальних слідів у соціальних мережах та на веб-сайтах в мережі Інтернет та інші способи пошуку інформації.

Программа X1 Social Discovery – створена для пошуку і збирання даних (медіа контенту Web даних) з соціальних мереж і Web-ресурсів (Facebook, Instagram, Twitter, YouTube, Tumblr, веб-сайтів, Gmail, YahooMail, Outlook.com, AOL Mail).

Програмне забезпечення **SMC4 Social Media Communication**, яке представляє собою інтегрований модуль програми **IBM i2** створене для дослідження зв'язків між акаунтами соціальних мереж Facebook, Twitter, Instagram та інших (LinkedIn, Google+ тощо) і здійснення онлайн моніторингу активності та публікацій користувачів цих соціальних мереж, а також побудови графічних схем зв'язків користувачів;

Використання:

- відкритих джерел інформації;

- спеціальних сервісів пошуку будь-якої інформації у соціальних мережах: (https://www.social-searcher.com, https://www.mediatoolkit.com/, https://namechk.com/);

- спеціальних сервісів, які дозволяють архівувати необхідний інтернет ресурс, роблячи його кеш-копію з можливістю подальшого використання (наприклад, http://web.archive.org/);

- можливостей **Graf Search** для отримання з мережі Facebook інформації про друзів, спільних друзів (https://www.faceboo.com/search/#FBID/friends; https://www.facebook.com/search/#FBID/followers; https://www.facebook.com/search /#FBID/users-followed) участі у групах (https://www.facebook.com/search /#FBID/groups, https://www.facebook.com/search/ #FBID/members), місцях (https://www.facebook.com /search/#FBID/places), лайки (https://www.facebook.com /search/#FBID/likes), коментарі до фото, відео тощо.

Враховуючи недостатній рівень знань слідчих та оперативних працівників у питаннях використання програмних засобів комп'ютерної техніки та мобільних пристроїв, відсутність уніфікованих методик, які дають можливість правильно та ефективно збирати цифрову інформацію, а також особливості цифрових джерел доказової інформації (можливість зміни характеристик і параметрів об'єктів, які фіксуються), їх вилучення з мобільних пристроїв (носіїв, ресурсів) має здійснюватися у присутності відповідного спеціаліста (наприклад, спеціаліста в галузі мережевих технологій, програмного (системного, прикладного) чи апаратного забезпечення тощо)) або спеціалістом*.

* У цьому розділі були використані відомості, представлені у презентаціях, що підготовлені фахівцями департаменту Кіберполіції та управління Кримінального аналізу Національної поліції України на теми: «Цифрові докази», «Організаційно-технічні особливості пошуку і вилучення електронно-обчислювальної техніки. Порядок огляду електронно-обчислювальної техніки. Порядок документального оформлення результатів пошуку, вилучення та огляду електронно-обчислювальної техніки», «Поняття кримінального аналізу, його види та роль у діяльності Національної поліції України».

РОЗДІЛ 9
МОЖЛИВОСТІ Й ПЕРСПЕКТИВИ АНАЛІЗУ ДАНИХ ПРО ПОДІЇ, ОСІБ ТА ЇХ ЗВ'ЯЗКИ У ПРОТИДІЇ ЗЛОЧИНАМ

Активність учасників злочинної діяльності та функціональні зв'язки між ними, як було відзначено у попередніх розділах, більшою мірою відображаються у здійснюваних телефонних дзвінках, комп'ютерних з'єднаннях і фінансових операціях. Збирання і аналіз такої інформації – необхідна складова виявлення, розслідування та попередження злочинів. Ефективність аналізу та синтезу отриманих відомостей багато в чому залежить від різноманітності доступних джерел інформації, повноти вихідних даних, а також застосованих технологій їх обробки.

Аналіз інформації щодо телефонних дзвінків та з'єднань дозволяє встановити:

- відомості про зв'язки абонентів і структуру злочинної групи;
- учасників злочинної групи, у тому числі раніше не відомих;
- порядок взаємодії між учасниками групи і орієнтовно – роль у злочинній діяльності;
- раніше не відомі епізоди злочинної діяльності;
- хронологію подій, які є предметом кримінальних проваджень, що розслідуються;
- приблизне місцезнаходження конкретного абонента в момент здійснення телефонного дзвінка або відправки SMS-повідомлення тощо;
- регулярні маршрути, за якими пересувається конкретний абонент. Зокрема, карти маршрутів – величезний простір для аналізу. Можна аналізувати щоденні та циклічні маршрути та відхилення від них, порівнювати ці маршрути із маршрутами потрібних абонентів. Таким чином, можна виявити можливі особисті безпосередні контакти з власниками інших номерів, їхню періодичність (перебування в безпосередній близькості в одному місці).

Для цього у клопотаннях про тимчасовий доступ до речей і документів (інформації, яка знаходиться у операторів і провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо), доцільно зазначати у них не тільки номери терміналів мобільного зв'язку, що належать або вилучені у підозрюваних, але і IMEI мобільних терміналів, якими вони користувалися, адже поширеною є практика, коли злочинці в конспіративних цілях часто змінюють різні SIM-карти у своїх телефонах. Це дозволить встановити всі номери, що були використані власником конкретного мобільного терміналу (телефону), визначити і відслідкувати всі зроблені за їх допомогою з'єднання.

Для можливості встановлення приблизного місцезнаходження конкретного абонента в момент здійснення телефонного дзвінка, що може мати доказове значення при встановленні обставин події кримінального правопорушення, необхідно у операторів телекомунікацій також отримати інформацію (роздруківку) про телефонні дзвінки із зазначенням дати, часу тривалості з'єднання, SMS та MMS-повідомлення, номери IMEI мобільних терміналів з прив'язкою до базових станцій та адреси їх розташування, дзвінки, під час яких з'єднання не відбувалось (нульові дзвінки), надання інших телекомунікаційних послуг, їх тривалості та маршрутів передавання, які фіксувалися конкретними базовими станціями оператора у конкретний день та час у вигляді роздруківки даної інформації та в електронному вигляді.

Інформація про з'єднання в мережі Інтернет вилучається з пам'яті терміналів мобільного зв'язку, планшетів, ноутбуків та інших електронних пристроїв, якими користувалися підозрювані. Додаткові відомості, у тому числі, про з'єднання осіб, з якими вони підтримували зв'язок, отримані від провайдерів послуг мережі Інтернет, можуть суттєво допомогти у встановленні структури та учасників злочинної групи. У цьому випадку в провайдерів

доцільно отримати відомості про час виходу в мережу Інтернет користувачів з відповідними акаунтами (логінами і паролями), їх IP-адреси, Log-файли з'єднань, відомості щодо використаних програм, зміст поштових скриньок, вхідні і вихідні повідомлення, збережені на сервері тощо.

Збираючи відомості про фінансову активність учасників злочинної діяльності, необхідно враховувати використаний ними спосіб збуту товарів, що заборонені або обмежені в обігу та розрахунків за них, а також схеми відмивання грошей, звертаючи увагу не лише на банківські рахунки осіб, але й електронні платіжні термінали різних платіжних систем, електронні гаманці, електронні гроші, про які йшла мова у розділі 2 рекомендацій. Отримати відомості про рух коштів по них можна в офісах відповідних компаній за запитами. Для зручності подальшого аналізу отриманих у такий спосіб матеріалів (інформації про телефонні з'єднання, інтернет-трафік, здійснені фінансові транзакції, у випадках, коли мова йде про довготривалу й систематично здійснювану злочинну діяльність) доцільно їх одразу вилучати в цифровому форматі на електронних носіях.

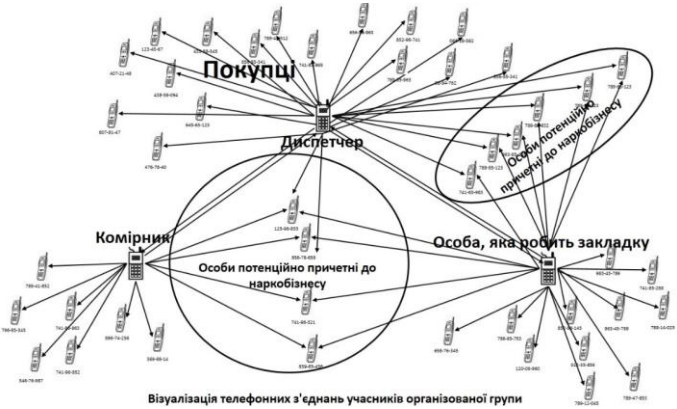
З метою пошуку доказової інформації з масивів отриманих від провайдерів відомостей рекомендується застосовувати метод аналізу даних, який проводиться за допомогою спеціальних комп'ютерних програм (наприклад, NetAnalysis, Analyst Notebook, Dr-Watson, XAMN Horizon, Maltego та ін.), робота яких заснована на візуалізації даних, автоматичному перетворенні в графічно оформлені семантичні мережі, «вузлами» яких є будь-які обрані об'єкти (люди, мережеві імена – «ніки», номери телефонів, IP-адреси, номери рахунків), а «нитками» - зв'язки між ними (телефонні дзвінки, сеанси зв'язку в Інтернеті, перекази грошей). Така технологія широко використовується в аналітичній розвідці[33], однак не є популярною серед слідчих та співробітників оперативних підрозділів.

[33] Бурьяк А. Аналитическая разведка. URL: http://analytical.narod.ru/Index.htm#1.

Доцільно розглянути можливості аналізу телефонних з'єднань на прикладі діяльності злочинної групи, що систематично здійснює «безконтактний» збут наркотичних засобів через «закладки». Цей спосіб скоєння злочинів розглядався нами в розділі 2 рекомендацій. Суть його полягає в тому, що замовлений у «оператора» по телефону або в мережі Інтернет наркотичний засіб оплачується покупцем шляхом внесення потрібної суми на електронний гаманець, пов'язаний з номером мобільного телефону, через платіжний термінал або іншим способом в мережі Інтернет, після чого йому повідомляється місце організації схованки - «закладки», де він може знайти і забрати своє замовлення, що залишив для нього «закладник». Безпосередній контакт між наркоторговцями і покупцями при такому способі збуту повністю виключається.

Численні злочинні групи, які здійснюють збут наркотичних засобів таким «безконтактним» способом, зазвичай мають загальне керівництво, систему комунікацій (загальні «торгові майданчики», закриті чати в мережі Інтернет тощо), поставки наркотичних засобів і грошових розрахунків, утворюючи цілі об'єднання злочинних груп. Схематично, механізм їх роботи можна представити таким чином (схема 1).

Графічна візуалізація телефонних з'єднань всіх учасників даної злочинної групи (схема 1) буде виглядати як представлено на схемі 2.



Візуалізація телефонних з'єднань учасників організованої групи

Отримана схема повністю відповідає вищеописаному механізму здійснення «безконтактного» збуту наркотичних засобів і наочно демонструє численні факти телефонних з'єднань, як між самими учасниками злочинної групи, так і покупцями наркотиків. Крім цього, стають відомими телефони інших потенційних підозрюваних: покупців наркотичних засобів і осіб, що неодноразово дзвонили відразу декільком учасникам злочинної діяльності, а значить, з високою ймовірністю, до неї причетних (великі «оптові» покупці, «бухгалтери», особи з інших угруповань) тощо.

Використання технології візуалізації результатів аналізу телефонних з'єднань для доведення факту вчинення злочину в складі групи є значно менш трудомістким і більш ефективним, аніж ручне порівняння і підрахунок телефонних з'єднань, що збіглися щодо осіб, які проходять по матеріалу провадження.

Звичайно, розглянутий приклад доволі простий. Структура зв'язків, телефонних з'єднань або фінансових операцій сучасної злочинної групи значно складніша. Крім того, такий аналіз частіше за все йде у «зворотному»

напрямі, не від готової схеми злочинного групи – до її підтвердження, а, навпаки, від телефонних з'єднань – до визначення структури і механізму злочинної діяльності. Однак візуалізація структури, як спосіб виявлення прихованої інформації, володіє достатньою універсальністю для дослідження матеріалів будь-якої складності.

Наступним прийомом отримання додаткової інформації з тих же даних є *накладення подій на шкалу часу*. Розглянути, як це працює, можна на тому ж спрощеному прикладі. Спосіб збуту наркотичних засобів «безконтактним» способом передбачає одну і ту ж послідовність дзвінків при вчиненні кожного наступного злочину. Так, при здійсненні роздрібного або дрібнооптового збуту покупець дзвонить «диспетчеру», той – «закладнику», а потім – у зворотному порядку, «закладник» повідомляє «диспетчеру», де він зробив закладку наркотичного засобу, а той передає покупцеві, де її знайти. При «оптовому» збуті картина може бути дещо іншою, оскільки у «закладника» може не виявитися в наявності достатньої кількості наркотичних засобів, «диспетчер» звернеться до «комірника», і той видає «закладнику» необхідну кількість товару. Так чи інакше, але в силу стійкості структури і складу учасників злочинної групи, а також «напрацьованості» способу вчинення злочинів, ці послідовності телефонних або інших з'єднань також є стійкими. Якщо «накласти» телефонні з'єднання фігурантів на шкалу часу, можна виявити аналогічні послідовності телефонних дзвінків за весь документований період їх діяльності. При цьому можна бути впевненим, що кожна з таких повторюваних послідовностей з великою часткою ймовірності може бути раніше невідомим або черговим епізодом збуту наркотичних засобів.

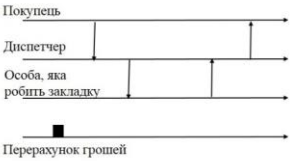
На сьогодні ні для кого вже не є сумнівом, що будь-який злочин, що вчиняється за допомогою засобів зв'язку, в тому числі мережі Інтернет, залишає свій специфічний «малюнок» слідів комунікації у вигляді характерної послідовності

контактів його учасників між собою. Цей слід, який визначається способом вчинення злочину, стійкий і може бути використаний для виявлення злочинів та їх учасників автоматично, наприклад, в ході моніторингу комунікаційного середовища спеціальною програмою. Схематично результати можна представити таким чином (схема 3).

Телефонні комунікації в організованій групі при збуті наркотиків

Схема комунікацій в організованій групі при оптовому збуті наркотиків

Схема комунікацій в організованій групі при роздрібному збуті наркотиків



Для підтвердження цієї версії можна також накласти на шкалу часу факти надходження грошей на рахунок, який використовується злочинцем для розрахунків з покупцями. При точній синхронізації часових шкал та ретельному вивченні інтервалів часу за датою, днями тижня, кількістю днів між подіями і часом доби, коли події відбувалися, виявляється, що всякий раз, в проміжок часу між дзвінком покупця і дзвінком «диспетчера» із зазначенням про «продаж товару», на цей рахунок надходить сума, кратна вартості разової дози споживання наркотичного засобу.

Отримана у такий спосіб інформація далеко не завжди може бути використана для доведення конкретних епізодів збуту наркотичних засобів, оскільки на момент розслідування, збуті раніше наркотичні засоби в більшості випадків вже будуть спожиті. Однак ніщо не перешкоджає використовувати ці дані для виявлення фактів торгівлі наркотичними засобами, а також для доведення стійкості злочинної групи, систематичного характеру

вчинюваної нею злочинної діяльності та орієнтовного підрахунку (виходячи з отриманих злочинних доходів) кількості збутих наркотичних засобів.

Наступним, рідко застосовуваним прийомом аналізу даних, *є накладення адрес подій на карту з* використанням Microsoft Excel або іншої програми, *з подальшим співставленням місць вчинення злочинів, проживання та затримання підозрілих осіб*[34]. В цьому контексті також може проводитися «географічний аналіз збуту наркотичних засобів, який дозволяє дослідити їх походження на певних ділянках місцевості (районах) для визначення особливостей і умов їх появи в обігу, взаємозв'язку протиправної діяльності та районів її здійснення, сприятливих і несприятливих чинників»[35]. В якості моделі-замінника зазвичай використовується мапа. А для наповнення карти необхідною інформацією використовують спеціальні символи – умовні знаки (*на карту* на прикладі вчинених грабежів) (мал. 1.).

[34] Поняття кримінального аналізу та його роль у системі Національної поліції України: план-конспект. Київ, 2018. С. 5-6.

[35] Купрієнко Д.А., Фаріон О.Б. Методологічні основи розвідувального аналізу в оперативно-розшуковій діяльності прикордонних підрозділів щодо протидії незаконним збройним формуванням при проведенні антитерористичної операції. *Збірник наукових праць Харківського університету Повітряних Сил*. 2016. Випуск 1(46). С. 154.

У такий же спосіб може здійснюватися накладення на карту телефонного трафіку, аналіз якого дозволяє вивчати напрями інформаційного обміну за телефонними каналами зв'язку – з метою виявлення взаємозв'язків між об'єктами уваги, що дозволяє окреслити географічний діапазон залучених в мережу абонентів, розкрити нових або невідомих учасників телефонних розмов[36] або встановити приблизне місцезнаходження конкретного абонента під час розмови і напрямок його руху. Система мобільного зв'язку обслуговується мережею базових станцій, з якими, при здійсненні дзвінка, зв'язуються мобільні термінали абонентів. Тому для визначення місця знаходження абонента необхідно за ухвалою суду отримати в компаніях, що надають послуги мобільного зв'язку відомості про з'єднання абонентів і абонентських пристроїв з урахуванням їх «прив'язки» до базових станцій.

Слід враховувати, що положення мобільних терміналів зв'язку щодо базових станцій фіксується не тільки в момент телефонної розмови або прийому-передачі даних (SMS, підключення мобільного Інтернету і т.п.), але й під час відправки базовою станцією службового сигналу у формі невидимого службового повідомлення, про що йшла мова у розділі 1 рекомендацій. А оскільки на базових станціях мобільного зв'язку використовуються спрямовані антени, при аналізі може бути встановлений сектор, в межах якого знаходився абонент в момент зв'язку його телефону з мережею.

Якщо в цей момент абонент рухався, переміщаючись від зони прийому однієї базової станції до іншої, можуть бути встановлені вектор і швидкість його переміщення. У містах базові станції стільникового зв'язку часто розта-

[36] Купрієнко Д.А., Фаріон О.Б. Методологічні основи розвідувального аналізу в оперативно-розшуковій діяльності прикордонних підрозділів щодо протидії незаконним збройним формуванням при проведенні антитерористичної операції. *Збірник наукових праць Харківського університету Повітряних Сил.* 2016. Випуск 1(46). С. 154.

шовуються настільки щільно, що абонент може бути одночасно зареєстрований відразу на декількох з них. Це дає можливість більш точного визначення його місця розташування (мал. 2).

Отримана інформація може мати доказове значення. Так, відповідність змісту розмови місцезнаходженню або напрямку руху абонента може підтверджувати факт його присутності на місці події, руху в напрямку місця розташування схованки, транспорту, що перевіз наркотичний засіб, зброю, заздалегідь обумовленого місця зустрічі зі співучасниками або покупцями заборонених або обмежених до обігу предметів, речовин тощо.

Подібним чином може бути проаналізований як телефонний, так і інший (наприклад, фінансовий) трафік. У такий спосіб також можуть бути встановлені переміщення особи і здійснювані нею дії на підставі інформації про використання кредитних карток у магазинах і банкоматах, платіжних терміналах, паркувальних автоматах та інших автоматичних пристроях.

Накладення розслідуваних подій «на карту» істотно полегшується за рахунок застосування сучасних можли-

востей спеціальних додатків (GIS-програм), що працюють в мережі Інтернет*. Такі програми, як GoogleMaps, GoogleEarth та інші, дозволяють отримати картографічне зображення будь-якої місцевості в необхідному масштабі з зазначенням об'єктів, що знаходяться на мапі. Карта «в один клік» може бути перетворена в супутниковий, аерофотознімок, або в тривимірну модель місцевості і розташованих на ній будівель.

Деякі програми дозволяють навіть моделювати природне освітлення на обраній ділянці місцевості в залежності від пори року, дня і стану атмосфери.

Сучасні додатки містять панорамні фотозображення картографічних об'єктів, дозволяють створювати ефект присутності в даній місцевості на екрані комп'ютера і «переміщатися» по ній, що надає нові можливості для попередження, виявлення й розслідування злочинів.

Для прикладу наведемо випадок з судової практики сусідньої з нами держави. *Так, наприклад, в ході допиту наркокур'єра, який контрабандним способом доставив велику партію особливо-небезпечного наркотичного засобу, замаскованого в конструктивних елементах свого автомобіля, підозрюваний погодився дати свідчення про місце, де його автомобіль був завантажений наркотиками. Точної адреси він не пам'ятав, однак заявив, що може показати це місце (металевий ангар) на карті й докладно описав його зовнішній вигляд. В умовах неможливості проведення слідчого експерименту з підозрюваним, для перевірки його показань, слідчий використав програму Google Maps, з використанням якої під час допиту завантажив на монітор панорамні зображення населеного пункту, про який говорив*

* GIS-додатки – комп'ютерні геоінформаційні системи, містять картографічне зображення місцевості, доповнене інформацією про необхідні об'єктах. Дозволяє користувачеві шукати, аналізувати і редагувати як саму цифрову карту місцевості, так і інформацію про об'єкти.

підозрюваний. Вивчаючи віртуальну модель міста, підозрюваний впевнено вказав не тільки на місце, де був розташований ангар, але і будинки інших учасників злочинної діяльності і навіть готель, де він зупинявся сам, поки його машину обладнали схованкою і завантажували наркотик, що надало слідчому нові докази протиправної діяльності причетних до злочину осіб.

ДОДАТКИ

Зразки документів

Запит на встановлення інформації про користувача IP-адреси

[реквізити підрозділу]
_____20__року № _____
На № _____ від _____

Директору_____філії
ПАТ «Укртелеком»
_____

Шановний _____!

У зв'язку з виконанням окремого доручення слідчого №_____ від 201_ року по кримінальному провадженню № _____від 201_ року, відкритого за ознаками злочину, передбаченого ч. 2 ст. 307 Кримінального кодексу України, на підставі ст. 23 Закону України «Про Національну поліцію», ст. 41 Кримінального процесуального кодексу України прошу Вас надіслати на адресу Управління / Відділу відомості щодо абонентів (у тому числі номери телефонів та IMEI мобільних терміналів), які для з'єднання з глобальною мережею Інтернет використовували наступні IP-адреси:

1. _____ – __.__.20__ о 22:55:12;
2. _____ – __.__.20__ о 21:45:11;
3. _____ – __.__.20__ о 20:35:10;
4. _____ – __.__.20__ о 19:25:09;
5. _____ – __.__.20__ о 18:15:15;

Враховуючи вкрай обмежений термін на проведення заходів, прошу сприяння у наданні зазначеної інформації в якомога стислий строк.

З повагою,
начальник управління / відділу _____

Вик. _____ _._.
тел. ___.__.__
т.м. _____

Запит про власника електронної поштової адреси

[реквізити підрозділу]
_____20__року № _____
На № _____ від _____

ТОВ «Реєстратор»
вул. Богомольця, 1, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження №_____від 20__ року, на підставі *посилання на статтю нормативно-правового акту,* прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який зареєстрував та використовує електронну поштову скриньку _____@ukr.net.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

Начальник управління / відділу _____

Вик. _____ _._.
тел. ___.__.__
т.м. _____

Запит про користувача IP-адреси

[реквізити підрозділу]
_____20__року № _____
На № _____ від _____

ТОВ «Інтернет Провайдер»
вул. Хрещатик, 10, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____від __.__ 20___, на підставі *посилання на статтю нормативно-правового акту,* прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який *дата* для доступу до всесвітньої інформаційної системи загального доступу Інтернет використовував IP-адресу***.***.***.***.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

Начальник управління / відділу _____

Вик. _____ _._.
тел. ___.__.__
т.м. _____

Запит про власника домену

[реквізити підрозділу]
_____20__року № _____
На № _____ від _____

ТОВ «Хостинг»
вул. Хрещатик, 10, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання но статтю нормативно-правового акту,* прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який протягом *період часу* використовував (-є) сервер (мережне обладнання) з IP-адресою ***.***.***.*** для розміщення на ньому сайту *домен* (лише у випадку послуг VPS-хостингу), а також інформацію про внесення зазначеним клієнтом оплати за отримані телекомунікаційні послуги. У разі наявності відповідних договорів або бухгалтерських документів прошу надіслати їх ввірені копії.

Заховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

Начальник управління / відділу _____

Вик. _____ _._.
тел. ___.__.__
т.м. _____

Список використаних джерел:

1. Бочковий О.В. Блокчейн відкритого суспільства, або реальні здобутки віртуального середовища. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. № 2. С. 69-77.

2. Бродський Ю.Б., Молодецька К.В., Пількевич І. А. Обчислювальна техніка та програмування. Ч. І. Інформатика та обчислювальна техніка: навч. посіб. Житомир: Вид-во ЖДУ ім. І. Франка, 2014. 204 с.

3. Бурьяк А. Аналитическая разведка. URL: http://analytical.narod.ru/Index.htm#1.

4. Використання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, їх транспортних телекомунікаційних мережах, під час розслідування злочинів: метод. рек. / С.С. Чернявський, О.Ю. Татаров, Д.О. Алексєєва-Процюк та ін. Київ: Нац. акад. внутр. справ, 2013. 69 с.

5. Виявлення, документування та розслідування злочинів, передбачених ст. 315 КК України, вчинених з використанням мережі Інтернет : навчально-практичний посібник / В.М. Комарницький, В.О. Криволапчук, Б.І. Бараненко та ін.; МВС України, Луган держ ун-т внутр. справ ім. Е.О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е.О. Дідоренка, 2017. 505 с.

6. Вознюк А.А., Алексєєва-Процюк Д.О. Використання ОВС можливостей операторів мобільного зв'язку під час розкриття та розслідування злочинів. *Криміналістика XXI століття*: матер. міжнар. наук.-практ. конф., 25-26 листоп. 2010 р. Харків: Право, 2010. С. 107-109.

7. Гогов Р.А. Методика расследования преступлений, связанных с незаконным оборотом наркотических средств, совершаемых организованными группами: дис… канд. юрид. наук: 12.00.09. Москва, 2010. 256 с.

8. Жуковський Т. Фіксування контенту веб-сторінки як доказу в судовому процесі. *Юридична практика.* 2013. № 39. С. 40-41.

9. Зеров К.О. Фіксація змісту веб-сторінки в мережі Інтернет як елемент здійснення права на захист авторських прав на твори, розміщені в мережі Інтернет. *Адвокат.* 2015. № 2. С. 17-22.

10. Ишин А. М. Современные проблемы использование сети Интернет в расследовании преступлений. *Вестник Балтийского федерального университета им. И. Канта.* 2013. Вып. 9. С. 116-123.

11. Іванов Г.В., Карасюк В.В., Гвозденко М.В. Основи інформатики та обчислювальної техніки: підручник / за заг. ред. В.Г. Іванова. Харків: Право, 2015. 312 с.

12. Карчевський М.В. Можливості Big Data та кримінально-правова комунікація. *Матеріали Міжнародної науково-практичної конференції «'Політика в сфері боротьби зі злочинністю».* Івано-Франківськ, 2017. С. 52-58.

13. Карчевський М.В. Особливості кримінально-правової кваліфікації злочинів проти власності, що вчиняються з використанням комп'ютерної техніки. *Діяльність підрозділів карного розшуку Національної поліції України щодо протидії злочинам проти власності, особливо корисливо-насильницьким у сучасних умовах*: збірн. матер. постійн. діюч. семінару (м. Миколаїв, 1-3 червня 2017 р.); за ред.: д.ю.н., проф. В.М. Комарницького, к.ю.н., доц. С.А. Комісарова, к.ю.н., проф. Б.І. Баранєнка. Сєвєродонецьк: Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка, 2017. С. 15-19.

14. Кваліфікація та розслідування злочинів, пов'язаних із незаконним збутом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет: метод. реком. / О.Ю. Татаров, О.М. Стрільців, В.Б. Школьний та ін. Київ: ГСУ МВС України, Нац. акад. внутр. справ. 2012. 30 с.

15. Коваленко А.В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України № 1 (88) 2017*. С. 182-191.

16. Козинкин В. А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: монография. Москва: Издат «Юрлитинформ», 2010. 192 с.

17. Кривонос М.В., Бондар В.С. Теорія та практика використання спеціальних знань в розслідуванні злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: монографія; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Сєвєродонецьк: РВВ ЛДУВС ім. Е. О. Дідоренка, 2017. 412 с.

18. Купрієнко Д.А., Фаріон О.Б. Методологічні основи розвідувального аналізу в оперативно-розшуковій діяльності прикордонних підрозділів щодо протидії незаконним збройним формуванням при проведенні антитерористичної операції. *Збірник наукових праць Харківського університету Повітряних Сил*. 2016. Випуск 1(46). С. 151-156.

19. Куцевич М., Берзін П. Неправомірний випуск й використання електронних грошей, що вчиняються у системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації). *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2013. Вип. 4. С. 13-16.

20. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 9-те вид., переробл. та допов. Київ: Юридична думка, 2012. 1056 с.

21. Новейший словарь иностранных слов и выражений. Мн.: Харвест, Москва: ООО «Издательство АСТ», 2001. 976 с.

22. Основи інформатики: підручник / укл. І.О. Яковлева. Харків АПБУ, 2003. 186 с.

23. Ошлыкова Е. А. Методика расследования незаконного сбыта наркотических средств и поддержания государственного обвинения по уголовным делам данной категории: монография. Москва: Юрлитинформ, 2013. 196 с.

24. Положення про електронні гроші в Україні: Постанова Правління Національного банку України від 04.11.2010 № 481.

25. Поляков В.В., Кондратьев М.В. Криминалистические особенности бесконтактного способа совершения наркопреступлений. *Известия Алтайского государственного университета*. № 2 (86). Том. 1. 2015. С. 83-86.

26. Поняття кримінального аналізу та його роль у системі Національної поліції України: план-конспект для проведення лекційного заняття з керівництвом Департаментів Національної поліції України. Київ, 2018. 26 с.

27. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III. URL: http://zakon2.rada.gov.ua/laws/show/2121-14

28.Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова правління Національного банку України від 14.07.2006 N 267. URL: http://zakon3.rada.gov.ua/laws/show/z0935-06

29.Про інформацію: Закон України від 2 жовтня 1992 р. № 2658–XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12

30. Про судову практику в справах про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: Постанова Пленуму Верховного Суду України від 26 квітня 2002 року № 4 (зі змінами, внесеними постановою від 18.12.2009 № 16). URL: http://www.scourt.gov.ua/clients/vs.nsf

31. Прокопенко Н. М. Криміналістична характеристика та основні положення розслідування незаконного збуту наркотиків: дис. канд. юрид. наук: 12.00.09. Харків, 2014. 215 с.

32. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. / О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін. Київ, 2016. 56 с.

33. Ступаков О.С. Використання можливостей операторів мобільного зв'язку, виробників мобільних операційних систем під час розкриття та розслідування кримінальних правопорушень. *Вісник Академії адвокатури України*. 2013. № 3(28). С. 89-92.

34. Тагієв С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово національної школи суддів України*. 2013. № 2(3). С. 13-24.

35. Тверезовська Н.Т., Нєлєпова А.В. Інформаційні технології в агрономії: навчальний посібник. Київ: Центр учбової літ-ри, 2013. 282 с.

36. Тютюн Т.М. Узагальнення проблемних питань, які виникають при розгляді клопотань про тимчасовий доступ до речей і документів. URL: http://www.apcourtkiev.gov.ua/wp-content/uploads/ 2015 /07/12014-kr.pdf

37. Ухвала Сєвєродонецького міського суду Луганської області від 25 січня 2017 року по справі № 428/776/17 у провадженні № 1-кс/428/356/2017. URL: https://opendatabot.com/court/ 64816676-36d072a61dce d8f7cd16eb2937c431c9

38. Ухвала Солом'янського районного суду м. Києва від 25 березня 2014 року по справі № 760/6158/14-к. URL: http://www.reyestr.court.gov.ua/Review/49510022

39. Фінансова грамотність: навч. посібник / авт. кол.; за ред. д-ра екон. наук, проф. Т.С. Смовженко. Вид. 2-ге, випр. і доп. Київ, 2013. 311 с.

40. Шебалин А. В. Особенности этапа предварительной проверки материалов о незаконном сбыте наркотических средств, совершённым бесконтактным способом. *Актуальные проблемы борьбы с преступлениями и иными правонарушениями*: материалы тринадцатой международной научно-практической конференции. Ч 1. 2015. С. 150-154.

41. Шимон С. Електронні гроші: форма грошей чи майнові права вимоги?. *Юридична Україна*. 2015. № 9. С. 36–41;

42. Юридична енциклопедія: В 6 т. / редкол.: Ю.С. Шемшученко (голова редкол.) та ін. Київ: «Укр. енцикл», 1998. 744 с.

43. Semantrum – персональний сервіс моніторингу всіх типів ЗМІ та соцмедіа. URL: https://promo.semantrum.net/uk/2017/04/21/v-ukrayini-na-pochatok-2017-roku-narahovano-21-6-mln-koristuv achiv-internetu/

Науково-практичне видання

БАРАНЕНКО Борис Іванович,
БОЧКОВИЙ Олексій Васильович,
КОМАРНИЦЬКИЙ Віталій Мар'янович,
КРИВОНОС Максим Васильович

ДІЯЛЬНІСТЬ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Науково-практичні рекомендації

За редакцією авторів
Технічний редактор *М.В. Кривонос*
Комп'ютерне верстання *М.В. Кривонос*

Підписано до друку 04.06.2018.
Формат 60х84 1/16 Ум. друк. арк. 6,3.
Тираж 300 прим. Зам. № 0406-01.

Адреса редакції та видавця:
Луганський державний університет внутрішніх справ імені Е.О. Дідоренка,
вул. Донецька, 1, м. Сєвєродонецьк, Луганська область, Україна, 93401;
тел. (06452) 9-07-77; адреса електронної пошти: oonr_lduvs@meta.ua;
сайт: http://lduvs.edu.ua

Виготовлено згідно з наданим оригінал-макетом:
Поліграфічне підприємство СПД Румянцева Г.В.
вул. Бузника 5/1, м. Миколаїв, 54038
Свідоцтво МК № 11 від 26.01.2007