МВС України

Харківський національний університет внутрішніх справ

Кафедра кримінального процесу та організації досудового слідства
Кафедра криміналістики, судової експертології та домедичної підготовки
Науково-дослідна лабораторія з проблем розвитку інформаційних технологій
Кафедра інформаційних технологій та кібербезпеки
Кафедра оперативно-розшукової діяльності та розкриття злочинів

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ ОБІГОМ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН, ЇХ АНАЛОГІВ, ПРЕКУРСОРІВ, ОТРУЙНИХ, СИЛЬНОДІЮЧИХ РЕЧОВИН, ОТРУЙНИХ СИЛЬНОДІЮЧИХ ЛІКАРСЬКИХ ЗАСОБІВ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНШИХ ТЕХНОЛОГІЙ

Науково-методичні рекомендації
(на замовлення Головного слідчого управління
Національної поліції України)

Харків 2020

УДК 343.98: 343.575] (083.13) (477)
ББК 67.9 (4УКР) 623.20я7р
О-75

Укладачі:

Юхно Олександр Олександрович – завідувач кафедри кримінального процесу та організації досудового слідства Харківського національного університету внутрішніх справ, доктор юридичних наук, професор.

Матюшкова Тетяна Петрівна – доцент кафедри криміналістики та судової експертології Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент.

Гнусов Юрій Валерійович – завідувач кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент.

Носов Віталій Вікторович – професор кафедри кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук.

Коршенко Вадим Анатолійович – завідувач науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ, кандидат юридичних наук.

Заворіна Олена Петрівна викладач кафедри кримінального процесу та організації досудового слідства Харківського національного університету внутрішніх справ

Лисенко Андрій Миколайович – доцент кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент.

Загуменний Олександр Олександрович – ад'юнкт відділу організації освітньо-наукової підготовки Харківського національного університету внутрішніх справ,

Туренко Дар'я Вікторівна – ад'юнкт відділу організації освітньо-наукової підготовки Харківського національного університету внутрішніх справ.

О-75 **Особливості** розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, отруйних, сильнодіючих речовин, отруйних сильнодіючих лікарських засобів із використанням сучасних телекомунікаційних та інших технологій: науково-методичні рекомендації / О. О. Юхно, Т. П. Матюшкова, В. А. Коршенко та ін. За загальною редакцією доктора юридичних наук, професора О. О. Юхна. Видання друге, доповнене і перероблене [Серія «Бібліотека слідчого і детектива: проблеми кримінального процесу»]. На замовлення Головного слідчого управління Національної поліції України. Харків : Константа ; Харківський національний університет внутрішніх справ. 2020. 144 с.
ISBN 978-996-342-413-9

У методичних рекомендаціях наведено криміналістичну характеристику, механізм документування та розслідування безконтактних збутів наркотичних засобів через мережу Інтернет, зокрема з використанням телефонних дзвінків і Інтернет-месенджерів та здійснення «закладок». Наведено механізм документування та розслідування збутів наркотичних засобів через мережу Інтернет при здійсненні оплати за наркотичні засоби криптовалютою. Розкрито питання кримінальної відповідальності та правового регулювання встановлення коштів, здобутих від незаконного обігу наркотичних засобів чи психотропних речовин, їх аналогів, прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів у банківських установах, на підприємствах, організаціях та їх підрозділах, майна чи обладнання для виробничих чи інших потреб, придбаних за власні кошти, або фактів використання таких доходів (коштів і майна) з метою продовження їх незаконного обігу.

УДК 343.98: 343.575] (083.13) (477)
ББК 67.9 (4УКР) 623.20я7р

ЗМІСТ

Вступ

Незаконний обіг наркотиків і наркоманія стали досить розповсюдженими і стимулюють зростання злочинності, насильства, корупції та уражають людей незалежно від соціального стану, статі, релігії чи раси. Сьогодні вказана проблема тією чи іншою мірою торкнулася практично всіх країн. Відповідно до Всесвітньої доповіді ООН з наркотиків у 2017 році 29,5 млн. людей у світі (0,6% від дорослого населення Землі) страждали на фізичні або психічні розлади, пов'язані з уживанням наркотиків, включно із залежністю. Не стала винятком і Україна. Так, за даними МВС в Україні налічується біля 500 тисяч наркозалежних, включно з тими, хто перебуває на поліцейських обліках, у зв`язку з немедичним уживанням наркотиків. Із них 171,6 тисяч уживають наркотики регулярно. Біля 5 тисяч наркозалежних є за віком до 18 років. За дослідженням міжнародних і національних громадських організацій встановлено, що 50% українських підлітків мають досвід куріння, 86% – вживали алкоголь, а 18% – наркотики. Згідно дослідження 12,3% підлітків мають доступ до марихуани, 7,1 % – до транквілізаторів, 5,8% опитаних підлітків заявили, що їм легко дістати амфетамін та крек, 5,2% – екстазі, 4,9% – метамфетамін, 4,3%- кокаїн, 4,2% – метадон.

Отже, наркотична ситуація в країні демонструє загальну тенденцію до погіршення, навіть незважаючи на скорочення території обліку, за рахунок тимчасово окупованих територій АР Крим і окремих районів Донецької та Луганської областей. Причому, починаючи з 1994 по 2020 рік відбулося майже трикратне зростання кількості наркозалежних. Наркоманія й злочинність є негативними продуктами соціальної дійсності, тісно взаємопов'язаними та такими, що взаємопроникають один в одного. Тому зміни в стані одного явища відбиваються на стані іншого. У сучасних умовах традиційні причини, що зумовлюють порушення соціальних норм, доповнюються, посилюються й ускладнюються кризовими явищами в економіці, соціальною нестабільністю, аморальністю та правовим нігілізмом. Відповідно, зміни, що відбуваються в усіх сферах життєдіяльності нашого суспільства, підіймають перед соціально-

гуманітарними науками, зокрема і перед кримінальним процесом, криміналістикою і кримінологією, завдання щодо вдосконалення форм і методів протидії негативним соціальним девіаціям, особливо наркотизму, та формування якісно нових стратегій й тактики правозастовного впливу, зокрема й з боку слідчих та оперативних підрозділів.

Нестабільність економічного та суспільно-політичного життя країни, різке зниження життєвого рівня населення, деградація традиційних моральних устоїв, пропаганда в засобах масової інформації різних форм девіантної поведінки, а також низка інших факторів створили сприятливі умови для зростання наркотизму в Україні, в першу чергу серед молоді. Численні реформи, спрямовані на розвиток прогресивних суспільних відносин, викликали серед іншого й негативні наслідки у вигляді виникнення нових сфер прояву кримінальних тенденцій, пов'язаних з розповсюдженням наркотиків, зокрема з використання мережі Інтернет із розрахунками криптовалютою. Розширився перелік наркотичних засобів і психотропних речовин, які споживаються та збуваються, їх територія та коло осіб, залучених у незаконних обіг. Наркотики перетворилися на невід'ємну частину сучасної субкультури (злочинного світу). У зв'язку з вищезазначеним у правозастосовній діяльності виникають прикладні завдання з вирішення наявних проблем щодо реалізації заходів у межах стратегії і тактики протидії, викриттю та розслідуванню розповсюдження наркотиків, серед яких слід виокремити правові, правозастосовні й організаційні. Актуальність вказаного питання підтверджується й статистичними даними. Так, зокрема в 2014 році у провадженні слідчих знаходилось 4883 проваджень такої категорії, у 2015 році – 6026, у 2016 році – 6219, у 2017 році – 10872, у 2018 році – 11131. Така ж тенденція простежується й у наступні роки. В той же час має місце зниження рівня розкриття такої категорії кримінальних правопорушень. Особливе місце в криміналістичній характеристиці незаконного обігу наркотиків займає глобальна мережа Інтернет, в якій все не так однозначно і просто. Процес контролю і моніторингу незаконної інформації, зокрема щодо пропозицій на реалізацію наркотиків через мережу Інтернет є досить складним,

неефективним і загалом перебуває в зародковому стані. У більшості випадків він посягає на життя, здоров'я, права та свободи особи, оскільки фільтрації (а вона є необхідною для виявлення деяких фактів порушення закону), як правило, піддається весь цифровий контент у досліджуваній сфері. Також складно встановити географічне розташування зловмисників, оскільки сервер з незаконним контентом, може, наприклад, перебувати за океаном у Каліфорнії, а самі порушники – в Україні. Тому без належного міжнародно-правового регулювання про ефективний всеосяжний контроль мережі Інтернет поки що вести мову зарано. У зв'язку з перерозподілом власності і нерухомості, значним зростанням незаконної трансплантації органів і тканин людини значно збільшується кількість злочинів у правовідносинах з нерухомістю, спадкоємством та в інших сферах власності, в яких інколи вчиняються кримінальні правопорушення із застосуванням сильнодіючих засобів – отруйних речовин, зокрема й з боку родичів, знайомих спадкоємців. Вказані засоби, а також особи, які їх можуть реалізувати також відшукуються серед працівників фармакологічних і лікарських установ, криміногенно налаштованих осіб, зокрема й через мережу Інтернет.

Після першого видання науково-методичних рекомендацій з цього питання, на сьогодні законодавцем внесено певні та суттєві зміни в кримінальне процесуальне законодавство України, яким, зокрема, введено нових учасників кримінального провадження – дізнавачів, керівників органів дізнання, а також прийнято ряд міжвідомчих та відомчих нормативно-правових актів, що регулюють ряд правових, організаційних питань та механізмів щодо протидії таких видів кримінальних правопорушень й у сфері незаконного обігу наркотиків, а саме: їх збуту, в тому числі й через мережу Інтернет та ін. Вказане спонукало до необхідності переопрацювання та перевидання наступних науково-методичних рекомендацій.

Автори

1. Особливості розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій

1.1. Особливості криміналістичної характеристики злочинів, пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій

Використання всесвітньої мережі Інтернет, сучасних телекомунікаційних та інших технологій стало одним із новітніх способів незаконного обігу і розповсюдження наркотиків, причетними до якого стають, як правило, раніше судимі особи й організовані злочинні групи, що намагаються у такий спосіб приховати свою злочинну діяльність від правоохоронних органів, уникнути безпосереднього обміну наркотиків на гроші та, як наслідок, можливості бути затриманими «на гарячому». Виступаючи в якості організаторів злочинів, зазначені особи активно залучають до їх вчинення осіб, які мають спеціальні знання в галузі інформаційних технологій (наприклад, для створення веб-сайтів, блогів, телеграм-ботів, технічної підтримки їх функціонування та ін.), молодь з числа осіб, які мають високий рівень матеріального забезпечення та бажання активно урізноманітнити своє життя, «спробувати все», у тому числі й вчинення злочинів (для спілкування в Інтернеті із покупцями, для зняття з карткових рахунків перерахованих ними грошових коштів та передачі їх організаторам), наркозалежних осіб, а також осіб, раніше судимих за вчинення злочинів (зокрема, для розміщення «закладок»).

Злочинці використовують сучасні телекомунікаційні технології, зашифровані мережеві Інтернет ресурси, псевдоніми, кодові слова, дотримуються заходів конспірації, координують свої дії та здійснюють обмін інформацією за допомогою різних телекомунікаційних мереж і мобільних додатків (застосунків). Зазначені додатки мають властивості технології наскрізного шифрування, що дозволяє читати повідомлення лише учасникам

листування (наприклад, WhatsApp) або мають функцію «секретний чат», повідомлення в якому видаляються автоматично в залежності від часу, встановленого користувачем та на серверах листування теж не зберігається (наприклад, Telegram). Зазначене суттєвим чином ускладнює виявлення та розслідування досліджуваних кримінальних правопорушень.

Також особи, причетні до незаконного обігу наркотиків із використанням сучасних телекомунікаційних та інших технологій, активно використовують і здійснюють розрахунки за незаконні операції з наркотиками у грошових одиницях Національного банку (гривні), іноземній валюті та криптовалюті, а також легалізують отримані від збуту наркотиків грошові одиниці шляхом їх переводу у криптовалюту, у тому числі, з подальшою легалізацією через офшорні компанії.

Так, у 2017 році учасники злочинної групи організували на території Києва та області діяльність так званих «майнінгових ферм», доходи від яких мали надавати законний вигляд грошовим коштам, отриманим від реалізації наркотичних засобів[1].

Криптовалюта за своєю суттю це цифрові гроші, випуск та електронний облік яких заснований на технології блокчейн, яка являє собою побудований за певними правилами безперервний послідовний ланцюг блоків, що містять інформацію. Тобто вся інформація зберігається не в одному централізованому місці, а на безлічі електронних засобів, сполучених мережею Інтернет. Історія транзакцій в блокчейні відкрита всім учасникам системи і незмінна, при цьому всі користувачі залишаються анонімними і мають рівні статуси. Блокчейн можна представити у вигляді облікової книги записів про події у цифровому світі, єдиним способом змінити стан реєстру в якій – зробити транзакцію. При цьому записи в журнал транзакцій можуть вноситися тільки з відома більшості учасників мережі. Це означає, що не можна непомітно видалити транзакцію з

[1] Как разводят на биткоинах: украинцы зарабатывают и теряют целые состояния на криптовалюте // Антикор. 14 грудня 2017, 16:12. URL: https://m.antikor.com.ua/articles/209536-kak_razvodjat_na_bitkoinah_ukraintsy_zarabatyvajut_i_terjajut_tselye_sostojanija_na_kriptovaljute.

журналу або додати нову в його середину. Технологія блокчейну базується на спеціальних алгоритмах шифрування, які потребують відповідного програмного забезпечення та комп'ютерного обладнання.

В Україні, як і в більшості країн світу, статус криптовалют залишається невизначеним. Згідно роз'яснення Національного банку України, правова природа криптовалюти не дозволяє визнати її власне валютною цінністю, а лише грошовим сурогатом, що не має забезпечення реальною вартістю та не контролюється державними органами влади. Криптовалюта не може використовуватись фізичними та юридичними особами на території України в якості засобу розрахунку, оскільки це суперечить нормам українського законодавства. У той же час сам майнінг, як процес електронних обчислень, не заборонений.[2] Такі види діяльності, як купівля-продаж та майнінг криптовалюти, відсутні у Класифікаторі видів економічної діяльності (КВЕД), водночас, відсутня й заборона на операції з криптовалютами. Згідно зі ст. 42 Конституції України, кожен має право на підприємницьку діяльність, яка не заборонена законом. Листом Держстату від 05.10.2018 р. №14.4-09/435-18 рекомендовано класифікувати майнінг та реалізацію криптовалют за КВЕДом 64.19 «Інші види грошового посередництва», а торгівлю (обмін) криптовалютами — за КВЕДом 66.19 «Інша допоміжна діяльність у сфері фінансових послуг, крім страхування та пенсійного забезпечення». У 2018 році до Верховної Ради України було внесено проект Закону «Про стимулювання ринку криптовалют та їх похідних в Україні», який у серпні 2019 р. був відкликаний.

Анонімність розрахунків у криптовалюті створює передумови для їх використання з метою легалізації грошових коштів, отриманих злочинним шляхом, оплати заборонених до вільного обігу товарів, зокрема наркотиків, що

[2] Глушко С. Майнинг криптовалют в Украине: 2018 год может стать решающим // Судебно-юридическая газета. 09.01.2018. URL: https://sud.ua/ru/news/publication/114785-mayning-kriptovalyut-v-ukraine-2018-god-mozhet-stat-reshayuschim (дата звернення 01.11.2020).

визнано загрозливою тенденцією за результатами засідання Національного координаційного центру кібербезпеки при РНБО України ще у 2018 році.[3]

Таким чином, у механізмі незаконного обігу наркотиків, що вчиняється з використанням сучасних телекомунікаційних та інших технологій, знаходять відображення певні закономірності, що обумовлені такими обставинами: 1) злочинці безпосередньо не знайомі один з одним та можуть проживати у різних населених пунктах чи країнах. Окрім того, легалізація отриманих від незаконного обігу наркотиків коштів може відбуватись не у місці знаходження (перебування) збувальника, а в іншому місці (місцях); 2) злочинці спілкуються за допомогою різноманітних комп'ютерно-технічних засобів зв'язку, використовують спеціальні програми чи сервіси (у тому числі, телеграм-боти, електронну пошту, миттєву передачу повідомлень в режимі он-лайн через програми типу «ICQ», «Skype», «Viber», здійснюють переписку в режимі он-лайн у форумах (чатах) сайтів тощо); 3) збувальник і покупець не зустрічаються для передачі наркотиків та коштів «з рук в руки», використовуючи електронні перекази, інші види безготівкових розрахунків та систему «закладок»; 4) до традиційних слідів вчинення даних видів злочинів додаються так звані «віртуальні» (або «цифрові» чи «комп'ютерні») сліди.

Зазначені обставини значно ускладнюють процес розслідування та фіксації обставин підготовки і вчинення незаконного обігу наркотиків, унеможливлюють свідчення підозрюваних або свідків про особливості зовнішності збувальників наркотиків, а також їх впізнання. До того ж використання злочинцями сучасних телекомунікаційних та інших технологій, комп'ютерно-технічних засобів та мережі Інтернет в якості способу вчинення злочину вимагає від слідчого, детектива і працівника оперативного підрозділу не лише якісного володіння навичками поводження з комп'ютерною технікою та програмами, але й навичками пошуку, виявлення, фіксації та копіювання інформації, що міститься на комп'ютерах, смартфонах, різноманітних

[3] О. Турчинов: Розвиток ринку криптовалют не може залишатися поза увагою держави. URL: http://www.rnbo.gov.ua/news/2965.html (дата звернення 01.11.2020).

цифрових носіях інформації та телекомунікаційних засобах, на Інтернет-ресурсах тощо.

Типовий механізм збуту наркотиків через мережу Інтернет є таким:

1. Створення збувальником спеціального Інтернет-ресурсу для збуту наркотиків, або розміщення відповідних оголошень, пропозицій чи реклами на існуючому вебсайті у мережі Інтернет, на сторінці у соціальній комп'ютерній мережі, або створення чат-боту у месенджері Telegram.

Наприклад, у 2017 році в Харкові затримали чоловіка та жінку, які створили Інтернет-крамницю, через яку торгували наркотиками у мережі, отримуючи оплату на банківські картки[4].

Створення спеціального Інтернет-ресурсу для збуту наркотиків властиве організованим злочинним групам, до складу яких входять спеціалісти у галузі комп'ютерних технологій, які безпосередньо і виконують вказану роботу та відповідають за розміщення відповідного контенту, забезпечують інформаційну безпеку, здійснюють технічну підтримку роботи сайту тощо.

Розміщення відомостей є процес публікації електронної інформації за допомогою комп'ютерного пристрою (платформи), що має підключення до Інтернету та передає таку інформацію у вигляді пакетів даних, створюваних і оброблюваних на основі стандартів протоколу IP. Розміщення даних у вигляді тексту, аудіо-, відео- або графічних об'єктів, як правило, відбувається на власних або публічних Інтернет-ресурсах: сайт, форум, чат, блог, дошка повідомлень та ін.

Під пропозиціями придбати наркотики розуміють розміщення інформації (текстова, графічна чи будь-яка інша) про наявність у особи певних видів наркотиків, які у подальшому можуть буди продані та доставлені покупцю. У пропозиціях можуть зазначатись способи поставки наркотиків та система оплати. При цьому відомості про рекламу або пропозицію придбати наркотики можуть розміщатись як у відкритому, так і у завуальованому вигляді (останнє

[4] В Харькове накрыли интернет-магазин наркотиков // Сегодня. 15.06.2017 р.. URL: https://www.segodnya.ua/regions/kharkov/v-harkove-nakryli-internet-magazin-narkotikov - 1030432.html (дата звернення – 01.11.2020).

більш поширено). У завуальованому вигляді інформація про збут наркотиків може бути розміщена з використанням певних умовних термінів, наприклад, «конструктор Лего» – пристрій для виготовлення наркотиків, «сіль для ванн» – синтетичні наркотики; «легальні суміші», «легальні порошки», «рослинні препарати», «агрохімікати», «лабораторне обладнання та реактиви», тощо.

До складу так званого «конструктора Лего» входять: докладна інструкція з використання, легальні хімічні реактиви – гидроксид натрію, метіламін, этілацетат, – з використанням яких навіть в умовах звичайної кухні стає можливим за п'ять-шість годин синтезувати «важкі» наркотики. При цьому спеціаліст в галузі хімії готовий надати консультації он-лайн[5].

Окрім пропозицій про продаж наркотиків від окремих осіб конкретним адресатам під час безпосереднього спілкування у мережі Інтернет, у т.ч. на Інтернет-форумах, у соціальних комп'ютерних мережах тощо, на різноманітних сайтах може бути розміщена й пряма реклама наркотиків. Реклама придбання наркотиків – це текстова, графічна чи будь-яка інша інформація (дані) з описанням певних видів наркотиків, пропозицією їх придбання у будь-якій формі та будь-яким способом, що існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись на комп'ютерних платформах.

У 2019 році було викрито діяльність злочинної групи з 6 жителів Харкова і області (серед яких 31-річний організатор кримінального бізнесу зі збуту наркотиків через мережу Інтернет, який вже мав судимість за вчинення злочинів, пов'язаних з незаконним обігом наркотичних засобів і психотропних речовин, і 5 учасників віком від 25 до 36 років). За даними досудового розслідування, організатор розмістив у мережі Інтернет завуальоване оголошення, в якому пропонував працевлаштування за професією «кур'єр», і створив сайт-форум для пошуку потенційних покупців наркотиків і прийому замовлень. У кожного з учасників організованої групи були свої обов'язки: одні

[5] Идеальная площадка. Торговля наркотиками быстро переходит в Интернет // Корреспондент.net. 15.04.2015. URL: http://korrespondent.net/ukraine/events/3503719-ydealnaia-ploschadka-torhovlia-narkotykamy-bystro-perekhodyt-v-ynternet (дата звернення - 01.11.2020).

отримували замовлення, інші – передавали наркотики через схованки – «закладки». Організатор закуповував оптові партії наркотиків і передавав так званим оптовим закладникам, які знаходили місця для товару, ховали наркотики і разом з координатами передавали роздрібним торговцям. Ті, знайшовши «закладку», фасували речовини на дози і робили свої схованки, фото яких з відповідними координатами в подальшому і потрапляли до замовника. Оператор приймав замовлення, перевіряв надходження коштів і передавав клієнтам інформацію про місця схованок з наркотиками. Збут наркотиків таким чином відбувався через Інтернет, особистого спілкування не було. Замовлення приймали через сайт-форум, місця схованок повідомлялися через Інтернет-месенджери, гроші переводилися на електронні гаманці. Учасники групи отримували «зарплату» на банківську картку або через схованки готівкою.[6]

Створення чат-боту у месенджері Telegram набуває розповсюдження через можливість зробити його анонімним (що виключається у таких месенджерах, як Viber), відносну нескладність створення чат-бота у відносно нетривалий період часу (в середньому це вимагає кілька годин) для web-програміста, до якого звертаються злочинці.

Так, у 2020 році повідомлено про підозру у незаконному придбанні, зберіганні з метою збуту, а також збуті наркотичних засобів та психотропних речовин в особливо великих розмірах (ч. 3 ст. 307 КК України) членам організованої злочинної групи, які у період з квітня по грудень 2019 року займалися збутом особливо небезпечних наркотичних засобів та психотропних речовин через месенджер. За даними правоохоронців, також до злочинної діяльності залучалися неповнолітні, які за грошову винагороду робили на

[6] Справу організованої групи закладників наркотиків і психотропів, яка працювала через Інтернет-магазин, направлено до суду. Інформаційне Агенство Інтерфакс-Україна. 20.08.2019 р. // URL: https://ua.interfax.com.ua/news/general/608065.html (дата звернення 01.11.2020).

фасадах будинків написи з «рекламою» відповідної адреси створеної злочинцями групи у месенджері. [7]

2. Пошук особою, яка бажає придбати наркотики, відомостей про реалізацію наркотиків на різноманітних веб-сайтах. За необхідності, завантаження та встановлення на своєму комп'ютері спеціального Інтернет-браузера «Tor Browser», що дозволяє отримати доступ до прихованих Інтернет-сайтів з продажу наркотиків. Також слід відзначити, що інформацію про адреси Інтернет-ресурсів, адрес електронної пошти, шифри, умовні терміни, за допомогою яких можна зв'язатись зі збувальником наркотиків, майбутній покупець наркотиків може отримувати й від інших осіб, які вже раніше придбавали наркотики у такий спосіб.

3. Встановлення контакту із особою, яка збуває наркотики через мережу Інтернет та розмістила відповідне оголошення на Інтернет-ресурсі, шляхом переходу за посиланням, направлення електронного листа або повідомлення, у тому числі, з використанням умовних термінів, шифрів, посиланням на осіб (постійних «клієнтів»), через яких отримав інформацію про можливість такого способу придбання саме за конкретними даними збувальника, ін.

4. Узгодження питань про вид, обсяг наркотику, його ціну, спосіб і терміни оплати та передачі. Таке спілкування є взаємним, короткостроковим (у випадку одноразового збуту) чи тривалим (при постійних контактах певних осіб з метою систематичного збуту наркотиків) та може здійснюватись різними способами: в режимі он-лайн з використанням програм миттєвої передачі повідомлень (месенджерів) типу «ICQ», «Jabber», «Skype», «Viber», «WhatsApp», «Telegram» та інших, листування у форумах (чатах) чи за допомогою електронної пошти. В подальшому злочинці можуть підтримувати зв'язок та спілкуватись за допомогою рухомого (мобільного) зв'язку, для чого

[7] Організованій злочинній групі повідомлено про підозру у збуті наркотиків в особливо великих розмірах на Луганщині. Офіс Генерального прокурора. 10 червня 2020 р. URL: // https://www.gp.gov.ua/ua/regions_news_detail?_m=publications&_c=view&_t=rec&id=274611 (дата звернення 01.11.2020).

вони обмінюються номерами мобільних телефонів (телефонними номерами SIM-карток).

5. Здійснення покупцем передоплати, як правило, може здійснюватись одним із зазначених способів: а) поповнення рахунку вказаного збувальником телефонного номеру; б) повідомлення секретного коду ваучера поповнення рахунку шляхом SMS-повідомлення; в) здійснення банківського переказу на вказаний збувальником банківський рахунок; г) переказ коштів з банківського рахунку покупця на вказаний збувальником банківський рахунок або номер телефону з використанням банківської картки, у тому числі, віртуальної; д) сплата електронними платіжними засобами (наприклад, «QIWI», «PayPal»), у тому числі такими, статус яких не визначено (наприклад, «біткоїнами»).

Так, один зі збувальників використовував різні платіжні сервіси: «Global Money» – для замовлень наркотиків вагою до 5 г , а «Приват24» – для більш значних обсягів наркотиків.[8]

6. Після оплати покупець отримує від збувальника інформацію про місце, час та спосіб отримання наркотиків. Такі повідомлення про місце знаходження наркотику та спосіб його отримання також можуть бути відправлені різними способами: розмова **по телефону**, відправка текстової інформації чи фотографії про місце приховування наркотику **через Інтернет** чи **SMS-повідомлення**. В якості способу передачі наркотиків використовуються: постачання поштою, кур'єрською службою доставки або самостійне забирання покупцем наркотику із обумовленого місця, в якому збувальником або його співучасником заздалегідь здійснена так звана «закладка».

Так, у Харкові викрито діяльність групи осіб, які через спеціально-створену Інтернет-крамницю продавали наркотики, здійснюючи їх «закладку» після надходження оплати[9].

[8] Идеальная площадка. Торговля наркотиками быстро переходит в Интернет // Корреспондент.net. 15.04.2015 р. URL: http://korrespondent.net/ukraine/events/3503719-ydealnaia-ploschadka-torhovlia-narkotykamy-bystro-perekhodyt-v-ynternet (дата звернення 01.11.2020).

Протидію окресленому виду злочинів, можна умовно поділити на два напрями:

1. Шляхом здійснення взаємодії з підрозділами протидії кіберзлочинності та оперативно-технічними підрозділами НПУ. При цьому ініціатива у протидії даним злочинам переходить від слідчого, оперативних працівників Департаменту протидії наркозлочинності або карного розшуку до вказаних підрозділів, які за допомогою використання можливостей технічних засобів здатні отримати додаткову інформації про злочинців, їх дії тощо та задокументувати їх причетність до злочину.

2. Другий напрям є класичним у діяльності оперативних підрозділів щодо протидії наркозлочинності та полягає, насамперед, у використанні можливостей штатних та позаштатних негласних працівників. Зазначені особи перебуваючи безпосередньо в злочинному середовищі здатні отримувати інформацію про факти підготовки та вчинення злочинів у сфері обігу наркотиків, у тому числі, й безконтактних збутів наркотичних засобів через мережу Інтернет, здійснення телефонних дзвінків, використання месенджерів. Це обумовлено тим, що злочинцям крім вчинення збуту наркотичних засобів вказаним шляхом, необхідно вчиняти низку інших злочинів у сфері обігу наркотиків, а саме: придбання наркотичних засобів та прекурсорів для їх виготовлення, зберігання їх, виготовлення або виробництво наркотичних засобів, їх транспортування тощо. Увесь цей ланцюг злочинної діяльності, пов’язаний із залученням до неї значної кількості осіб, що у кінцевому підсумку призводить до витоку інформації про розглядувані злочини.

Працівникам оперативних підрозділів Департаменту протидії наркозлочинності, інших оперативних підрозділів та слідчим Національної поліції України з метою протидії вказаним вище злочинам доцільно відпрацьовувати наступні категорії осіб:

---

[9] В Харькове накрыли интернет-магазин наркотиков // Сегодня. 15.06.2017 р. URL: https://www.segodnya.ua/regions/kharkov/v-harkove-nakryli-internet-magazin-narkotikov - 1030432.html (дата звернення 01.11.2020).

1. Осіб, які незаконно вживають наркотики, не користуючись послугами наркоторговців. Такі особи самостійно придбають або виготовляють наркотичні засоби чи об'єднуються в групи споживачів для забезпечення себе наркотичними засобами, приєднуються з цією метою до інших неформальних об'єднань, фактично орієнтованих на їх вживання, виготовлення та збут.

2. Осіб, які незаконно вживають наркотики, користуючись послугами наркоторговців. Останні, в свою чергу, використовують цих осіб для роздрібної торгівлі наркотичними засобами та залучення інших осіб до немедичної вживання наркотиків.

3. Працівників науково-дослідних інститутів хімії, технологів, хіміків-лаборантів хімфармпідприємств, що мають справу з реактивами і прекурсорами, які можуть використовуватися як сировина для виготовлення синтетичних наркотиків.

4. Осіб раніше засуджених за вчинення злочинів у сфері обігу наркотиків.

5. Осіб, які притягувалися до адміністративної відповідальності за вчинення правопорушень у сфері обігу наркотиків.

6. Осіб з числа медперсоналу, які за своїми функціональними обов'язками мають доступ до наркотичних засобів.

7. Осіб циганської та кавказької національності.

8. Осіб, які незаконно вживають наркотики та є працівниками ІТ сфери, мають знання та навички використання комп'ютерних програм, мережі Інтернет, новітніх технологій.

Відповідно встановлювати конфіденційне співробітництво доцільно з особами, які мають довірливі, дружні або ділові зв'язки з переліченими вище особами.

Враховуючи вимоги чинного КПК України документування безконтактних збутів наркотичних засобів через мережу Інтернет, здійснення телефонних дзвінків, використання месенджерів здійснюється, як правило, оперативними працівниками за дорученням слідчого, (а у зв'язку із змінами в

чинному КПК України з 01.07. 2020 р.) ще й за дорученням дізнавача, начальника органу дізнання в межах кримінального провадження.

Як свідчить аналіз досвіду практичної діяльності протидії окреслиним видам злочинів, найбільш поширеними негласними слідчими (розшуковими) діями, які використовуються під час їх документування є: аудіо-, відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем, обстеження публічно недоступних місць, житла чи іншого володіння особи, установлення місцезнаходження радіоелектронного засобу, спостереження за особою, річчю або місцем, аудіо-, відеоконтроль місця та контроль за вчиненням злочину. Обрання методики документування даних кримінальних правопорушень, тобто послідовності проведення негласних слідчих (розшукових) дій залежить від конкретних обставин вчинення правопорушення, особистості злочинців та наявної оперативної інформації.

«Закладкою» наркотиків називають їх схованку у різноманітних безлюдних або прихованих від людської уваги місцях, якими можуть бути: поштовий ящик, батарея опалення, електричний або пожежний щиток у під'їзді багатоповерхового житлового будинку, клумба з квітами поблизу житлових будинків чи у парках (скверах), покриття та їх елементи гаражів, тощо. При цьому наркотик маскується або упаковується таким чином, щоб не привертати до себе уваги сторонніх і уникнення вилучення сторонніми особами, а вся координація дій і обмін інформацією між співучасниками, а також із замовником, здійснюється за допомогою телекомунікаційних мереж і мобільних додатків (застосунків), таких як «Telegram», «Viber», «WhatsApp», «Jabber», «Skype» та ін. Тому, з метою затримання осіб «на гарячому» при отриманні наркотиків із «закладок» необхідна розробка і реалізація комплексу оперативно-розшукових заходів чи оперативно-розшукових комбінацій, або тактичних операцій та ін. (методика, тактика, реалізація та деталізація чого відома і має інформацію з обмеженим доступом).

7. Отримавши наркотик, покупець вживає його або реалізує іншим особам (залежно від мети придбання та обсягів придбаної партії).

8. Особи, які вчиняють злочини, пов'язані із незаконним виробництвом, виготовленням, придбанням, зберіганням, пересиланням чи збутом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет, отримуючи грошові кошти через мережу задіяних осіб, відкритих карткових рахунків чи у інший спосіб, використовують їх у різноманітних, у тому числі, злочинних цілях. Зокрема, розраховуються зі співучасниками, витрачають грошові кошти на придбання, виготовлення чи виробництво нових партій наркотиків та ін. Непоодинокими є випадки, коли такі злочинні угрупування також придбають і зброю.[10]

Інформація про факти незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів, здійснюваний з використанням мережі Інтернет, може бути отримана правоохоронними органами з таких джерел: 1) слідчим під час розслідування інших злочинів у інших кримінальних провадженнях; 2) детективом чи працівником оперативного підрозділу під час проведення оперативно-розшукових заходів та від джерел оперативної інформації; 3) із заяв чи повідомлень громадян про виявлення у мережі Інтернет-сайтів, сторінок у соціальних комп'ютерних мережах із оголошеннями про продаж наркотиків.

Протидію розглядуваному виду злочинів, можна умовно поділити на два напрями:

Перший напрям реалізується шляхом здійснення взаємодії з підрозділами протидії кіберзлочинності та оперативно-технічними підрозділами поліції. При цьому ініціатива у протидії даним злочинам переходить від слідчого, детектива, оперативних працівників Департаменту протидії наркозлочинності або карного розшуку до вказаних підрозділів, які за допомогою використання можливостей

[10] Наркоторговцы занимались майнингом криптовалюты в Украине // Delo.ua. 22.01.2018 р. URL: https://delo.ua/ econonomyandpoliticsinukraine/narkotorgovcy-zanimalis-majningom-kriptovaljuty-338232 (дата звернення 01.11.2020).

технічних засобів здатні отримати додаткову інформації про злочинців, їх дії тощо та задокументувати їх причетність до злочину.

Так, за повідомленням НПУ, у такий спосіб співпраці між Кіберполіцією та підрозділами протидії наркозлочинності, за сім місяців 2019 року поліцейські викрили 255 фактів збуту наркотичних засобів та психотропних речовин з використанням Інтернету.[11]

Другий напрям є класичним у діяльності оперативних підрозділів щодо протидії наркозлочинності та полягає, насамперед, у використанні можливостей штатних та позаштатних негласних працівників (ст. 275 КПК України, ст. 8 Закону України «Про оперативно-розшукову діяльність»). Зазначені особи, безпосередньо перебуваючи в злочинному середовищі, здатні отримувати інформацію про факти підготовки та вчинення злочинів у сфері незаконного обігу наркотиків, у тому числі, й безконтактного збуту наркотичних засобів через мережу Інтернет. Це обумовлено тим, що злочинцям крім збуту наркотиків вказаним шляхом, необхідно вчиняти низку інших злочинів у сфері незаконного обігу наркотиків, а саме: придбання наркотичних засобів та прекурсорів для їх виготовлення, зберігання вказаних речовин, виготовлення або виробництво наркотичних засобів, їх транспортування тощо. Увесь цей ланцюг злочинної діяльності пов’язаний із залученням значної кількості осіб, що у кінцевому підсумку призводить до надходження д правоохоронних органів інформації про підготовку та вчинення досліджуваних злочинів. Використовувати довірливі, дружні або ділові зв’язки з метою встановлення конфіденційного співробітництва доцільно з особами, які найчастіше причетні до незаконного обігу наркотиків. А саме:

1) споживачами наркотиків, які не користуються послугами наркоторговців, самостійно придбають або виготовляють наркотичні засоби чи об’єднуються в групи споживачів для забезпечення наркотиками, приєднуються

[11] Кіберполіція та підрозділи протидії наркозлочинності співпрацюватимуть для припинення розповсюдження наркотиків через Інтернет. Урядовий портал. 06.09.2019 р. // URL: https://www.kmu.gov.ua/news/kiberpoliciya-ta-pidrozdili-protidiyi-narkozlochinnosti-spivpracyuvatimut-dlya-pripinennya-rozpovsyudzhennya-narkotikiv-cherez-internet (дата звернення 01.11.2020).

з цією метою до інших неформальних об’єднань, фактично орієнтованих на вживання, виготовлення та збут наркотиків;

2) споживачами наркотиків, які користуються послугами наркоторговців. Останні, в свою чергу, використовують таких споживачів для роздрібної торгівлі наркотиками та залучення до їх немедичного вживання інших осіб;

3) хіміки, технологи, хіміки-лаборанти хімфармпідприємств, науково-дослідних інститутів, які у своїй роботі використовують чи мають доступ до реактивів і прекурсорів, що можуть використовуватися як сировина для виготовлення синтетичних наркотиків;

4) раніше засуджені за злочини у сфері незаконного обігу наркотиків;

5) особи, які раніше притягувались до адміністративної відповідальності за вчинення правопорушень у сфері незаконного обігу наркотиків;

6) медичний персонал, що за своїми функціональними обов’язками має доступ до наркотичних лікарських засобів;

7) особи певного походження, які схильні до вчинення незаконного обігу наркотиків (відповідно до територіальних особливостей наявного населення або того, що мігрує між областями, наприклад, роми, представники народів, що проживають на Кавказі тощо).

8) працівники ІТ-сфери, які є споживачами наркотиків, що використовують наявні знання та навички у сфері інформаційних технологій для придбання чи (і) збуту наркотиків через мережу Інтернет.

Аналіз досвіду практичної діяльності правоохоронних органів щодо протидії незаконному обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів свідчить, що найбільш поширеними негласними слідчими (розшуковими) діями, які використовуються для фіксації злочинних діянь є: спостереження за особою, річчю або місцем, аудіо-, відеоконтроль особи та місця, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем, обстеження публічно недоступних місць, житла чи іншого володіння особи, установлення

місцезнаходження радіоелектронного засобу, контрольоване вчинення злочину у формі контрольованої поставки чи(і) контрольованої та оперативної закупки, ін.

Особливості документування незаконного обігу наркотиків, обрання послідовності проведення негласних слідчих (розшукових) дій залежить від конкретних обставин вчинення злочину, особистості злочинців, наявної оперативної інформації та інформації, що є в матеріалах конкретних оперативно-розшукових справ чи кримінальних проваджень.

АНАЛІЗ БІТКОЇН-ТРАНСАКЦІЙ В РОЗСЛІДУВАННЯХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЩОДО НАРКОТИКІВ ТА ІН.

Біткоїн – це незалежна криптовалюта з платіжною системою, в якій децентралізовані:

- емісія монет;
- підтвердження трансакцій;
- зберігання даних;
- аудит облікової системи;
- прийняття рішення щодо оновлень протоколів і програмного забезпечення.

Криптовалюти:

операють деякими цінностями, а не реальними валютами;

- не мають одного емітента – всі учасники системи за певним протоколом емітують нові цінності;
- є віртуальною готівкою, а не зобов'язанням емітента видати реальну валюту або оплатити товар онлайн;
- є протоколом (інструментом) для передачі цінності через комп’ютерні мережі;
- використовують криптографічні алгоритми цифрових підписів;
- можуть забезпечувати анонімність.

При розслідуванні кримінальних правопорушень, де фігурують криптовалюти, зокрема біткоїн, вхідним для аналізу є біткоїн-адреса.

Біткоїн-адреса – це ідентифікатор, з яким в розподіленій базі даних асоційований певний баланс біткоїн-монет.

На сьогодні біткоїн-адреси можуть бути представлені в двох форматах – Base58 і Bech32.

Адреса у форматі Base58 є усіченим результатом подвійного ґешування відкритого ключа володільця коштів за допомогою ґеш-функції SHA-256, і починається з 1 або 3, може містити від 27 до 34 літер і цифр латинського алфавіту різного регістру окрім 0, O, I (і велика), і l (L маленька). Приклад адреси:

`1NSV7yEvaJY4pVpLAbMhBjRQCugDDrnnWG`

Формат Base58 має певні обмеження:

- адреса в Base58 займає більше пам'яті в QR-кодах, оскільки не може використовувати режим буквено-цифрового подання;
- Base58 є дуже незручним для надійного запису на папір, введення з мобільного клавіатури або читання вголос;
- подвійне ґешування контрольної суми є повільним;
- декодування Base58 є складним і порівняно повільним.

На заміну формату Base58 був прийнятий формат Bech32. Адреса формату Bech32 має довжину, яка не перевищує 90 символів, і містить наступні складові.

- *Першу частину* з даними, зручними для читання людиною. Ці дані можуть бути певним повідомленням або мати якесь відношення до власника адреси. Довжина даних – від 1 до 83 символів. Наприклад, за замовчуванням для адрес mainnet (діюча мережа біткоїн) використовуються символи «bc», а для testnet (тестова мережа біткоїн) символи «tb».
- *Роздільник* – символ одиниці «1». Якщо «1» дозволена всередині першої частини, то роздільником є остання «1».
- *Другу частину* з даними довжиною не менше 6 символів. Абетка цієї частини складається тільки з букв і цифр, за винятком «1» (одиниця), «b», «i», і «o». В якості основних даних тут використовується версія witness program і дані самої witness program (від 2 до 40 байт).

Абетка із 32 символів для кодування даних за форматом Bech32 є такою:

q	p	z	r	y	9	x	8
g	f	2	t	v	d	w	0
s	3	j	n	5	4	k	
c	e	6	m	u	a	7	l

Приклади Bech32 біткоїн-адрес:

- Mainnet P2WPKH (Pay to Witness Public Key Hash): `bc1qw508d6qejxtdg4y5r3zarvary0c5xw7kv8f3t4`
- Testnet P2WPKH (Pay to Witness Public Key Hash): `tb1qw508d6qejxtdg4y5r3zarvary0c5xw7kxpjzsx`
- Mainnet P2WSH (Pay to Witness Script Hash): `bc1qrp33g0q5c5txsp9arysrx4k6zdkfs4nce4xj0gdcccefvpysxf3qccfmv3`
- Testnet P2WSH (Pay to Witness Script Hash):
- `tb1qrp33g0q5c5txsp9arysrx4k6zdkfs4nce4xj0gdcccefvpysxf3q0sl5k7`

Буквено-цифровий код біткоїн-адреси може бути перетворений у QR-код (рис. 1).

Мал. 1 – QR-код біткоїн-адреси

Для трати коштів з біткоїн-адреси (формування трансакції), у залежності від типу адреси, необхідно знання одного або декілька приватних (секретних) ключів.

Адресі, що починається з цифри 1, ставиться у відповідність один приватний (секретний) ключ, знання якого дозволяє підписувати трансакцію при траті коштів з цієї адреси.

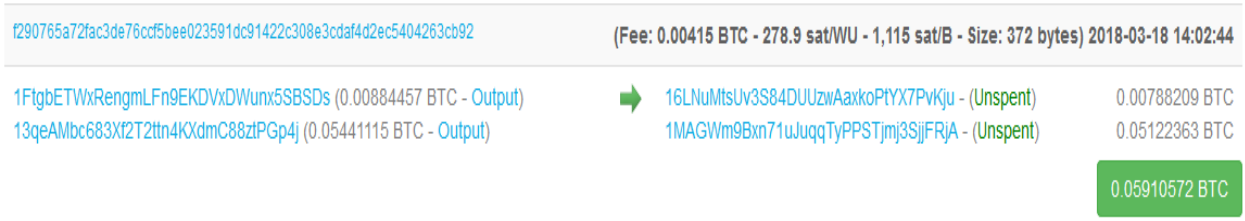
Адресі, що починається з цифри 3, поставлено у відповідність декілька приватних ключів. В цьому випадку у залежності від визначеного сценарію для

підпису трансакції потрібно використати або всі або певну кількість ключів з усіх.

Адреса є анонімною і не містить інформації про власника. Генерація адреси здійснюється відповідним програмним забезпеченням локально без підключення до мережі біткоїн.

Одна людина може мати необмежену кількість біткоїн-адрес. Кожний раз для отримання коштів можна створювати нову адресу. Програмне забезпечення біткоїн-гаманця може оперувати будь-якою кількістю адрес, або кожна адреса може обслуговуватися окремим гаманцем.

Усі затверджені трансакції (ті, що потрапили у блокчейн) у вигляді блоків із зазначенням суми, адреси-відправника і адреси-отримувача знаходяться у вільному доступі та доступні для ознайомлення на різноманітних ресурсах Інтернету (наприклад, blockexplorer.com, blockchain.info, live.blockcypher.com/btc, blocktrail.com/BTC і інші). Будь який користувач може завантажити увесь актуальний журнал біткоїн-трансакцій (блокчейн), що надає принципову можливість побудувати ланцюг руху коштів між різними біткоїн-адресами. На рис. 2 показана структура однієї із трансакцій.



Мал. 2 – Структура біткоїн-трансакції

З мал. 2 можна зазначити, що унікальний номер трансакції:

f290765a72fac3de76ccf5bee023591dc91422c308e3cdaf4d2ec5404263cb92,

імовірно одна людина (якщо не застосовувались засоби додаткової анонімізації) володіє двома рахунками з відповідними балансами:

1FtgbETWxRengmLFn9EKDVxDWunx5SBSDs (0.00884457 BTC),

13qeAMbc683Xf2T2ttn4KXdmC88ztPGp4j (0.05441115 BTC),

оскільки ініціює одночасно два перекази на два адреса, з яких монети ще не витрачені:

16LNuMtsUv3S84DUUzwAaxkoPtYX7PvKju – (Unspent) 0.00788209 BTC,

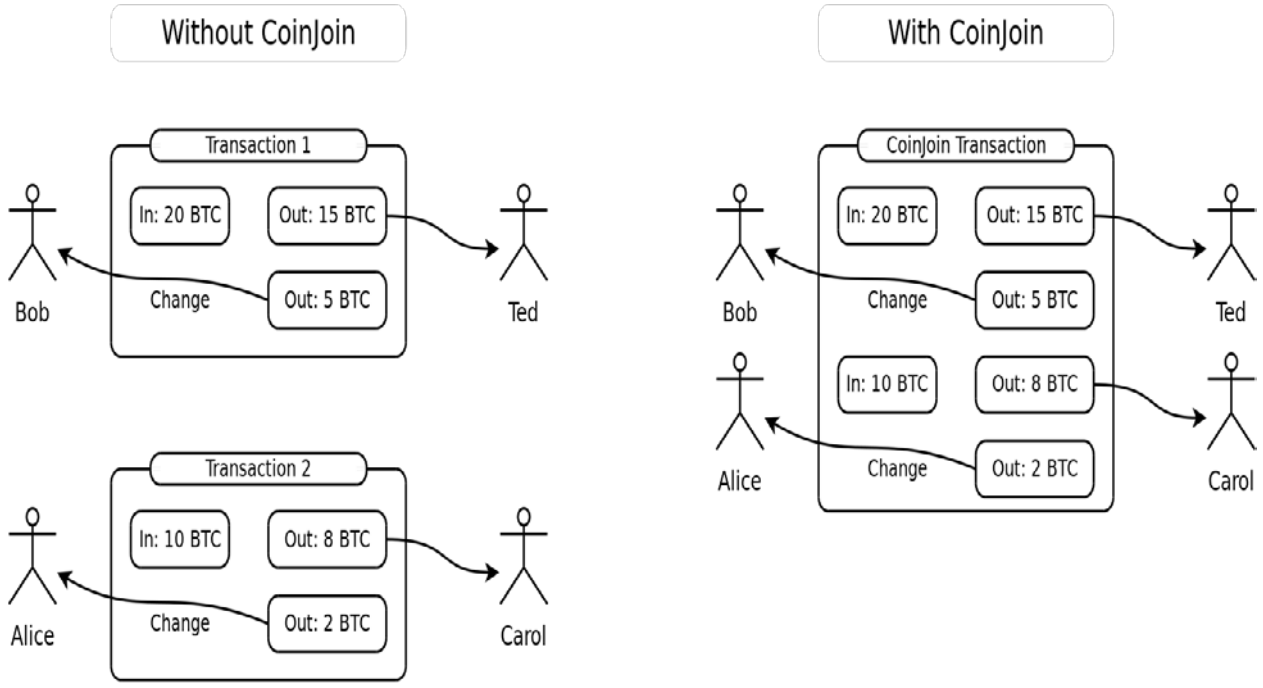
1MAGWm9Bxn71uJuqqTyPPSTjmj3SjjFRjA – (Unspent) 0.05122363 BTC.

Імовірно, що одна із адрес отримання, належить ініціатору трансакції, куди він перераховує остачу.

Таким чином, можна прослідити ланцюг руху коштів з виходу певної адреси на вхід іншої (інших).

З метою ускладнення аналізу біткоїн-трансакцій в глобальній мережі з'явилися ресурси, що пропонують послуги "мікшування" трансакцій шляхом прийняття спочатку на одну адресу або кілька адрес коштів від багатьох користувачів, а потім у випадковому порядку і з різною затримкою в різних трансакціях переказ коштів на адреси, що наперед визначені користувачами сервісу мікшування.

Також, існує метод підвищення анонімності CoinJoin, який не потребує наявності третьої довіреної сторони, а передбачає об'єднання переказів в одну трансакцію від декількох користувачів (мал. 3).



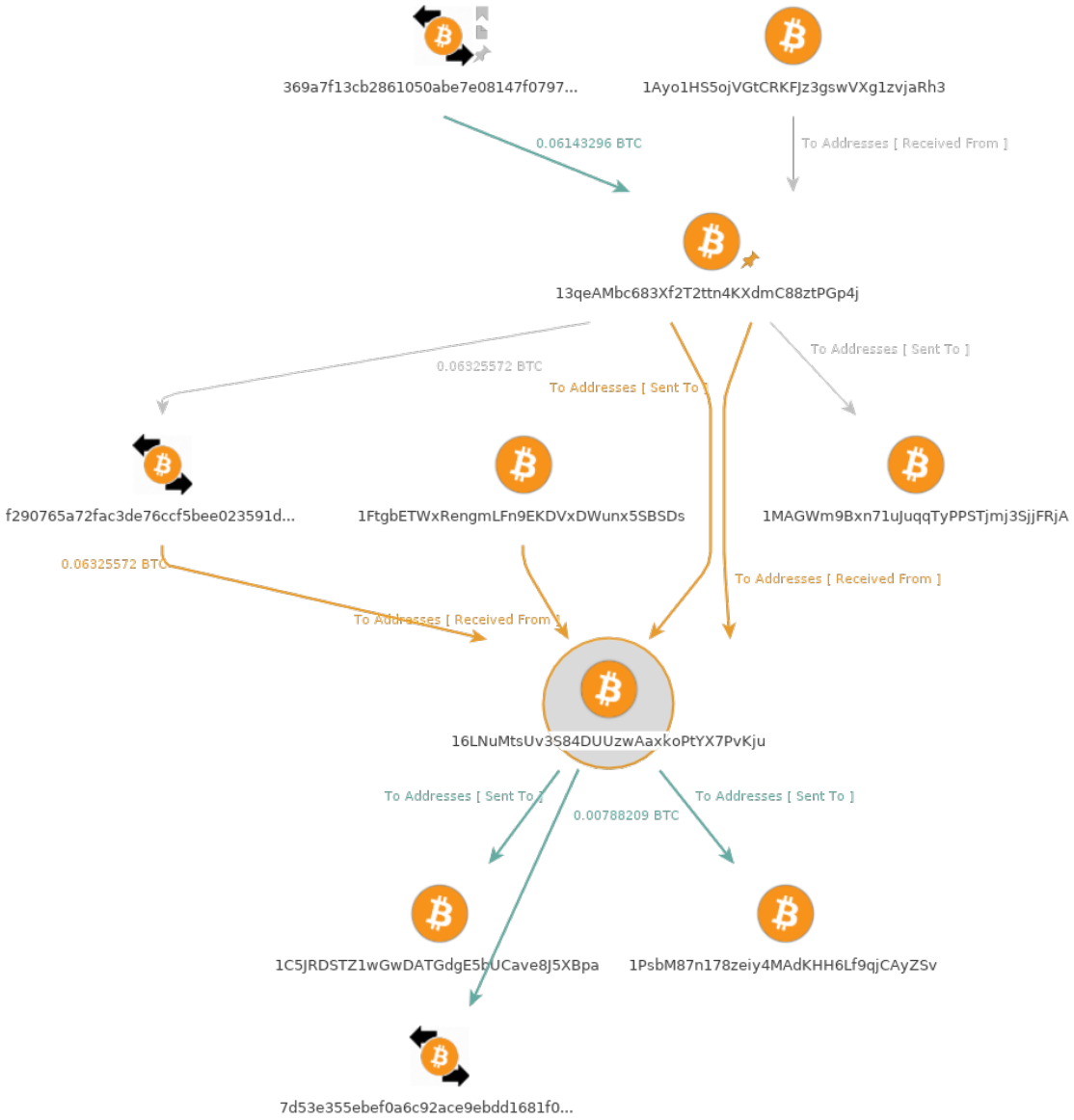
Мал. 3 – Логічна структура CoinJoin об'єднання переказів в одну трансакцію від декількох користувачів (https://en.wikipedia.org/wiki/CoinJoin)

Наявні біткоїн-адреси за допомогою пошукових сервісів можна зв'язати із:

- IP адресою;
- доменним ім'ям;
- електронною поштою;
- обліковим записом користувача якого-небудь сервісу;
- ідентифікатором соціальних мереж;
- тощо.

Анонімність біткоїн-адреси втрачається при обміну монет біткоїн на фіатну (звичайну) валюту в обмінних сервісах, біржах та ін.

У якості засобу автоматизації пошуку та побудови схеми відношень різних ідентифікаторів біткоїн-трансакцій можна використовувати безкоштовну програму Maltego Community Edition (maltego.com) із встановленим трансформатором аналізу біткоїн ідентифікаторів. Приклад побудови логічної схеми трансакцій між певними адресами наведений на мал. 4.



Мал. 4 – Приклад побудови логічної схеми трансакцій між певними адресами в Maltego Community Edition

Також на ринку спеціалізованого програмного забезпечення пропонуються комерційні застосунки (сервіси) аналізу трансакцій і адресів криптовалют.

Одним із таких сервісів є платформа аналізу криптовалют від компанії Crystal Blockchain (crystalblockchain.com).

Потреби розслідувань кримінальних правопорушень цілком задовольняє версія сервісу Crystal Expert, користування яким здійснюється через веб доступ (програма як послуга, SaaS).

На листопад 2020 року в Crystal Expert пропонується аналіз:

- Bitcoin (BTC);
- Bitcoin Cash (BCH);
- Ethereum (ETH);
- Ethereum tokens: ERC20 & ERC721;
- Litecoin (LTC);
- Tether (USDT);
- Ripple (XRP).

Основною аналітичною цінністю сервісу Crystal Expert є база ідентифікованих та неідентифікованих володільців (entities) біткоїн-адрес, що підтримується у актуальному стані. В поточному стані база містить 2908 володільців біткоїн-адрес (Bitcoin Entities), які розділені на наступні 19 типів.

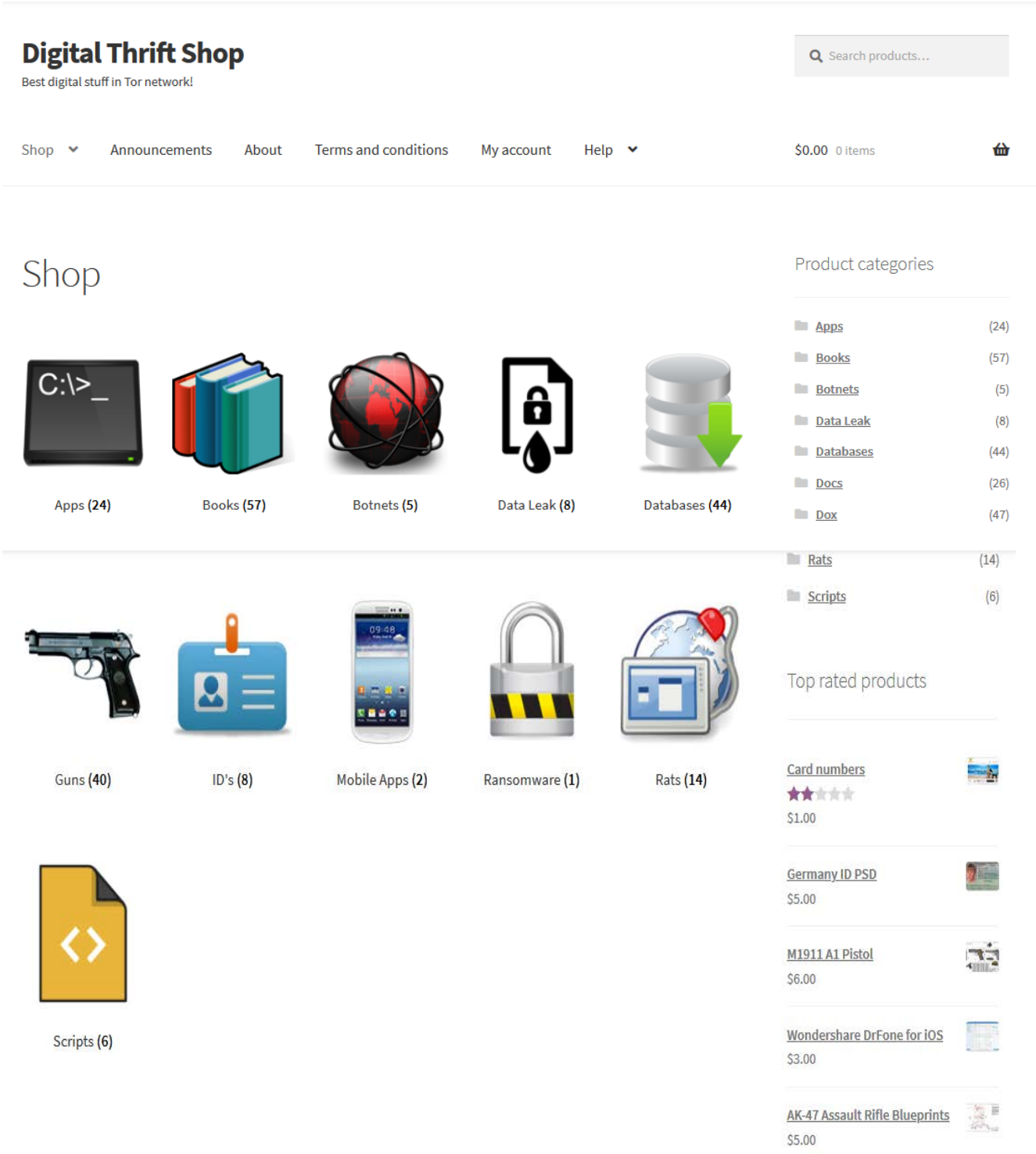
1. Автомати покупки/продажу біткоїн (ATM, 19 мереж), наприклад, BitRocket (www.bitrocket.co, 1543 біткоїн-адреси, мал. 5), Athena Bitcoin (www.athenaбіткоїн.com, 176 біткоїн-адреси, мал. 6), які розташовані в різних країнах світу.

Мал. 5 – BitRocket автомат покупки/продажу біткоїн

Мал. 6 – Athena Bitcoin автомат покупки/продажу біткоїн

2. Кримінальні торгові майданчики в TOR мережі (Darknet Marketplace, 305 майданчиків), наприклад, Digital Thrift Shop (26 біткоїн-адреси, мал. 7) – поточна адреса в TOR мережі:

kw4zlnfhxje7top26u57iosg55i7dzuljjcyswo2clgc3mdliviswwyd.onion.



Мал. 7 – Фрагмент стартової вебсторінки кримінального торгового майданчика Digital Thrift Shop

3. Суб'єкти надання нелегальних послуг за криптовалюту через TOR мережу (Darknet Service, 34 entities), наприклад, Abrisk (156 біткоїн-адрес), Card OK (250 біткоїн-адреси), PinPays (1 656 679 біткоїн-адреси), CC Clinique (147 874 біткоїн-адреси).

4. Криптовалютні біржі з *високим ризиком* відмивання грошей (Exchange With High ML Risk, 98 бірж), наприклад, BtcTurk (www.btcturk.com, 140 170 біткоїн-адреси), SpectroCoin (spectrocoin.com, 174 094 біткоїн-адреси), Coinbase (www.coinbase.com, 47 747 018 біткоїн-адреси).

5. Криптовалютні біржі з *низьким ризиком* відмивання грошей (Exchange With Low ML Risk, 147 бірж), наприклад, Bittrex (global.bittrex.com, 1 741 608 біткоїн-адреси), Kraken (www.kraken.com, 1 431 475 біткоїн-адреси), Bitso (bitso.com, 1 392 066 біткоїн-адреси).

6. Криптовалютні біржі з *помірним ризиком* відмивання грошей (Exchange With Moderate ML Risk, 28 бірж), наприклад, LocalБіткоїns (localбіткоїns.com, 8 870 868 біткоїн-адреси), Huobi (www.huobi.com, 2 165 049 біткоїн-адреси), Paxful (paxful.com, 1 318 502 біткоїн-адреси).

7. Криптовалютні біржі з *дуже високим ризиком* відмивання грошей (Exchange With Very High ML Risk, 232 бірж), наприклад, Yobit (yobit.net, 1 094 881 біткоїн-адреси), Kucoin (www.kucoin.com, 653 125 біткоїн-адреси), Changelly (changelly.com, 647 117 біткоїн-адреси).

8. Шахрайські обмінники криптовалют (Fraudulent Exchange, 6 обмінників), наприклад, BTC-e (btc-e.com, 775 161 біткоїн-адреси).

9. Сайти азартних ігор, де приймається і виплачується криптовалюта (Gambling, 105 сайтів), наприклад, Bovada (www.bovada.lv, 2 478 796 біткоїн-адреси).

10. Нелегальні сервіси з оплатою криптовалютою (Illegal Service, 43 сервіси), наприклад, CamGirl247 (camgirl247.com, 72 067 біткоїн-адреси), Raccoon Stealer (поширення шкідливих програм, 369 біткоїн-адреси), Dailystormer (пропаганда нацизму, 163 біткоїн-адреси).

11. Майнери криптовалют (Miner, 102 майнери), наприклад, NiceHash (www.nicehash.com, 139 479 біткоїн-адреси), Eligius (eligius.st, 133 810 біткоїн-адреси).

12. Сервіси мікшування біткоїн-трансакцій для підвищення анонімності володільців біткоїн-адрес (Mixing Service, 31 сервіс), наприклад, Wasabi wallet (wasabiwallet.io, 2 364 336 біткоїн-адреси).

13. Легальні онлайн сервіси надання послуг, пов'язаних із криптовалютою (Online Marketplace, 9 сервісів), наприклад, Purse (purse.io, 35 307 біткоїн-адреси), eMoney (www.emoney.ge, 92 175 біткоїн-адреси).

14. Сервіси онлайн гаманців біткоїн (Online Wallet, 47 сервісів), наприклад, blockchain.info (11 645 365 біткоїн-адреси), Cryptonator (www.cryptonator.com, 1 230 548 біткоїн-адреси).

15. Некласифіковані сервіси, що пов'язані з криптовалютою (Other, 150 сервісів), наприклад, Bitmain Hardware (bitmain.com, апаратні та програмні рішення із підтримки blockchain, 101 045 біткоїн-адреси), MoonБіткоїн (moonbit.co.in, система оплати за виконання онлайн завдань, 49 898 біткоїн-адреси), BitVPS (bitvps.com, оренда віртуальних виділених серверів, 22 700 біткоїн-адреси).

16. Системи обробки криптовалютних платежів (Payment Processor, 28 процесорів), наприклад, CoinPayments (coinpayments.net, 5 614 908 біткоїн-адреси), GoCoin (gocoin.com, 4 857 420 біткоїн-адреси).

17. Програми-вимагачі криптовалют (Ransom, 790 програм), наприклад, Cerber Ransomware (шкідлива програма шифрування даних із вимаганням викупу, 8 838 біткоїн-адреси), Locky Ransomware (шкідлива програма шифрування даних із вимаганням викупу, 7 552 біткоїн-адреси), Petya (шкідлива програма шифрування даних із вимаганням викупу, 1 біткоїн-адреса)..

18. Шахрайські ресурси, пов'язані із криптовалютами (Scam, 638 ресурсів), наприклад, HashOcean (hashocean.support, 1 190 477 біткоїн-адреси), Bitconnect.co (503 378 біткоїн-адреси), MisterTango (mistertango.com, 22 187 біткоїн-адреси).

19. Біткоїн-адреси, на які виводились вкрадені біткоїн монети (Stolen Coins, 96 випадків), наприклад, Bitfinex Thief 2016 (крадіжка з біржі Bitfinex в 2016 р., 2 072 біткоїн-адреси), NiceHash Thief 2017 (крадіжка з майнінгового сервісу NiceHash в 2017 р., 125 біткоїн-адреси), Zaif Thief 2018 (крадіжка з криптовалютного обмінника Zaif в 2018 р., 78 біткоїн-адреси).

В Crystal Expert кожному типу володільця (entity type) або володільцю біткоїн-адрес (entity) призначається або розраховується оцінка ризику (Risk

Score) щодо імовірної участі у кримінальній діяльності і кримінальності походження коштів. За умовчанням для 18 типів володільців біткоїн-адрес (окрім типу "Other") створений вихідний профіль шкали оцінки ризику (Risk Score Profile, табл. 1), в якому також встановлюється ступінь впливу категорії на оцінку ризику для неідентифікованих володільців біткоїн-адрес – якщо кошти надійшли з біткоїн-адрес цієї категорії (Receiving direction) та якщо кошти були відправлені на біткоїн-адреси цієї категорії (Sending direction). З вихідного профілю користувач сервісу може створювати власний, в якому можна змінювати:

- величину ризику категорії (Risk Score) – від 0% до 100%;
- ступінь впливу на оцінку ризику неідентифікованих володільців біткоїн-адрес за напрямами: прийом коштів з категорії; відправлення коштів до категорії:
    - не впливає (none);
    - слабо (low);
    - середньо (medium);
    - сильно (high).

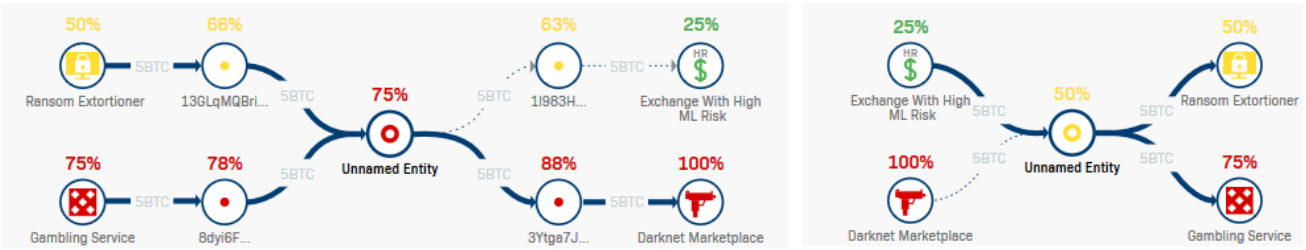
Таблиця 1. Вихідний профіль шкали оцінки ризику (Risk Score Profile)

№	Entity type	Risk Score	Receiving direction	Sending direction
1.	ATM	50%	High	High
2.	Darknet Marketplace	100%	High	High
3.	Darknet Service	100%	High	High
4.	Exchange With High ML Risk	50%	High	High
5.	Exchange With Low ML Risk	0%	High	High
6.	Exchange With Moderate ML Risk	25%	High	High
7.	Exchange With Very High ML Risk	50%	High	High
8.	Fraudulent Exchange	75%	High	High
9.	Gambling	75%	High	High
10.	Illegal Service	100%	High	High
11.	Miner	0%	High	High
12.	Mixing Service	100%	High	High
13.	Online Marketplace	0%	High	High
14.	Online Wallet	25%	High	High
15.	Payment Processor	0%	High	High
16.	Ransom	100%	High	High
17.	Scam	100%	High	High
18.	Stolen Coins	100%	High	High

Налаштування власного профілю шкали оцінки ризику дозволяє враховувати особливості розслідування. Наприклад, для визначеного на мал. 8 профілю шкали оцінки ризику, величина ризику неідентифікованих володільців біткоїн-адрес (Unnamed Entity), які отримують і відправляють кошти через проміжні біткоїн-адреси, показана на мал. 9. Зміна профілю шкали оцінки ризику (мал. 10) призводить до зміни величини ризику для тих же неідентифікованих володільців біткоїн-адрес (мал. 11).

Entity type	Risk Score	Receiving direction	Sending direction
Darknet Marketplace	100%	None	High
Exchange With High ML Risk	25%	High	None
Gambling	75%	High	High
Ransom	50%	High	High

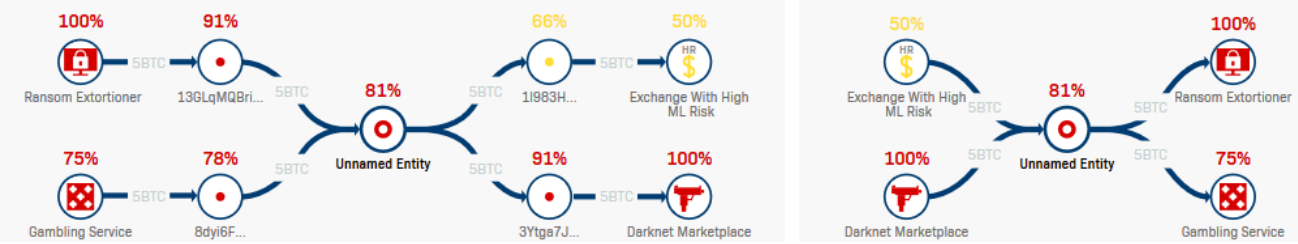
Мал. 8 – Тестовий профіль №1 шкали оцінки ризику



Мал. 9 – Обчислений згідно тестового профілю №1 (рис. 8) ризик неідентифікованих володільців біткоїн-адрес (Unnamed Entity)

Entity type	Risk Score	Receiving direction	Sending direction
Darknet Marketplace	100%	High	High
Exchange With High ML Risk	50%	High	High
Gambling	75%	High	High
Ransom	100%	High	High

Мал. 10 – Тестовий профіль №2 шкали оцінки ризику

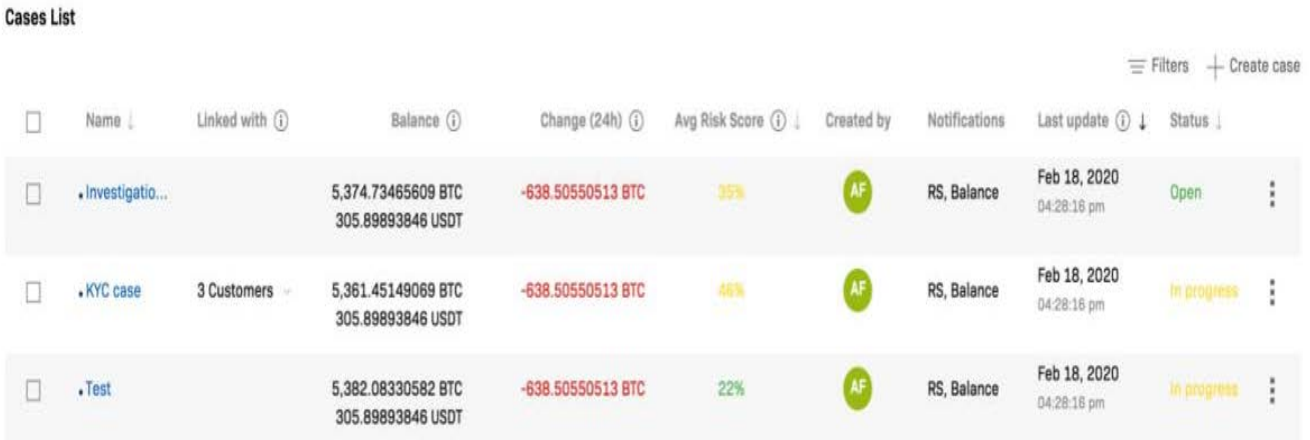


Мал. 11- Обчислений згідно тестового профілю №2 (мал. 10) ризик неідентифікованих володільців біткоїн-адрес (Unnamed Entity)

Crystal Expert містить 5 основних (мал. 12) і 2 додаткових інструменти розслідування.

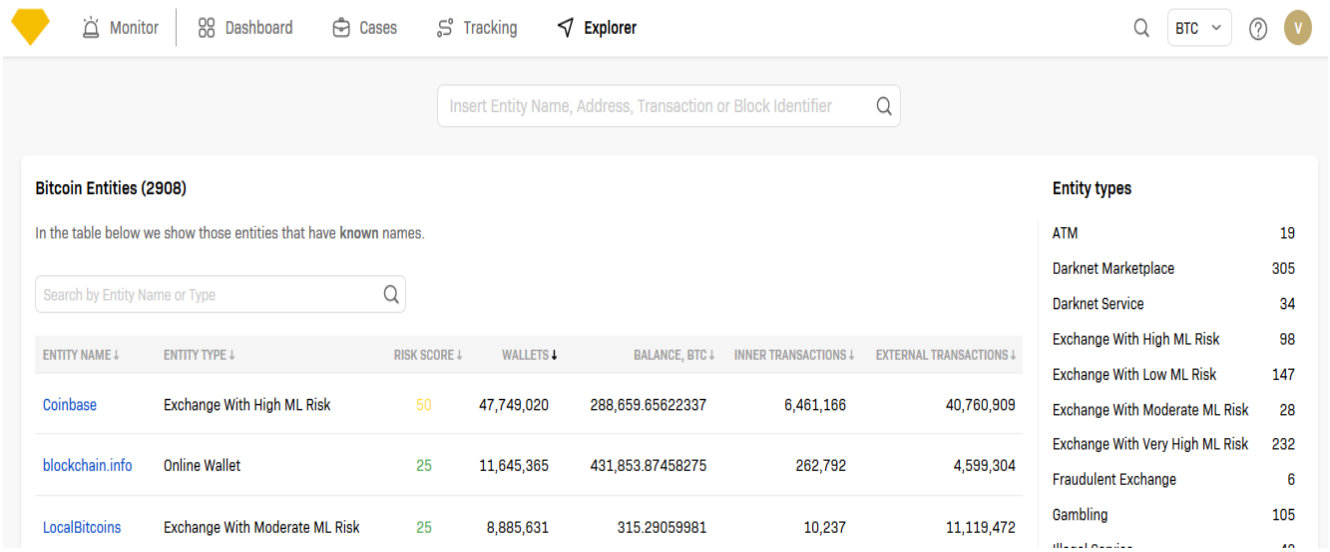
Мал. 12 – Панелі основних інструментів розслідування

Інструмент **"Справи (Cases)"** призначений для управління розслідуваннями у вигляді справ. Тут можна створювати нові справи і переглядати поточні (мал. 13). Сторінка справи містить основні деталі, адреси, візуалізації та відстеження, додані до справи.



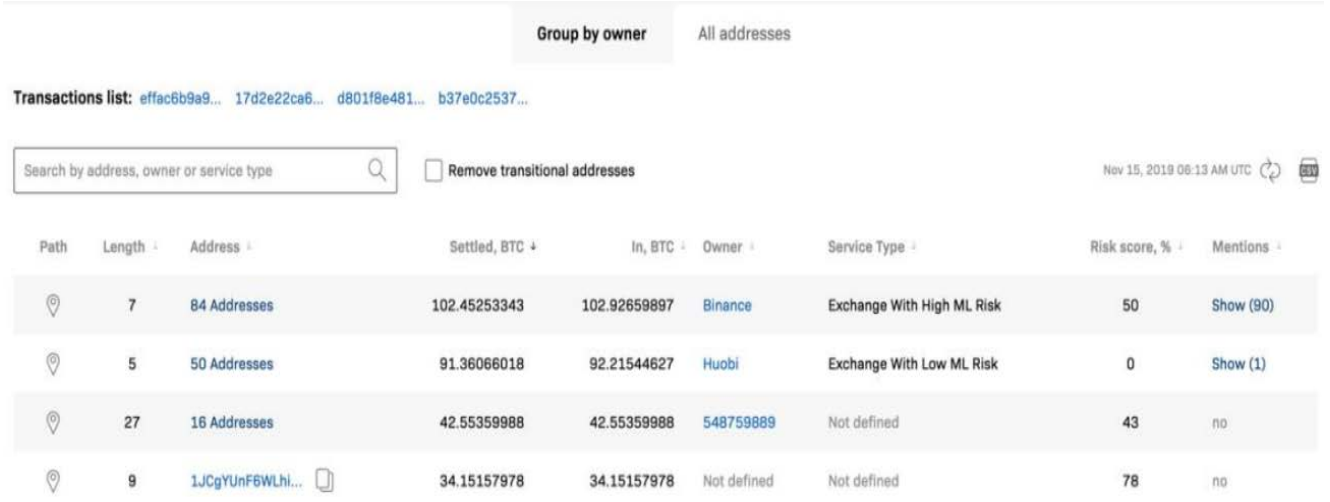
Мал. 13 – Поточні записи інструменту "Справи (Cases)"

Інструмент **"Дослідник (Explorer)"** призначений для дослідження трансакцій, блоків та адрес, а також відображення інформації про ідентифікованих володільців біткоїн-адресів, їх типів (мал. 14), основних майнерів та курс біткоїна.



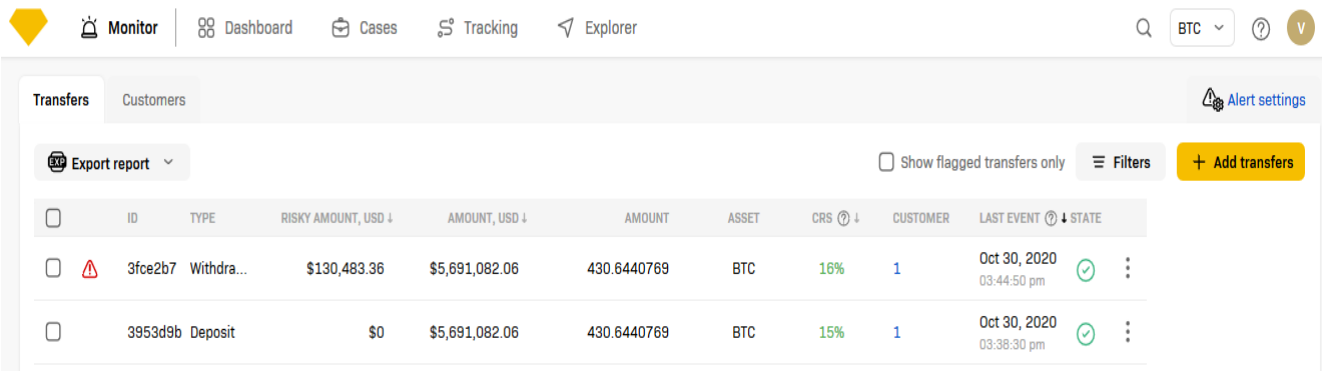
Мал. 14 – Фрагмент початкової сторінки інструменту "Дослідник (Explorer)"

Інструмент **"Відстеження (Tracking)"** дозволяє відстежувати у часі подальший рух коштів за визначеною трансакцією або групи трансакцій (мал. 15). Відстеження може виявити, чи потрапили вихідні кошти з визначеної трансакції до ідентифікованого володільця біткоїн-адрес, наприклад, біржі або платіжного процесора, що, в свою чергу, може дозволити ідентифікувати через відповідні правові процедури власника вихідної біткоїн-адреси.



Мал. 15 – Фрагмент результатів відстеження визначених трансакцій інструменту "Відстеження (Tracking)"

Інструмент **"Монітор (Monitor)"** в основному призначений для compliance-офіцерів фінансових інституцій, дозволяє за налаштованими правилами перевіряти ступінь ризикованості (Risk Score) певних трансакцій (мал.16).

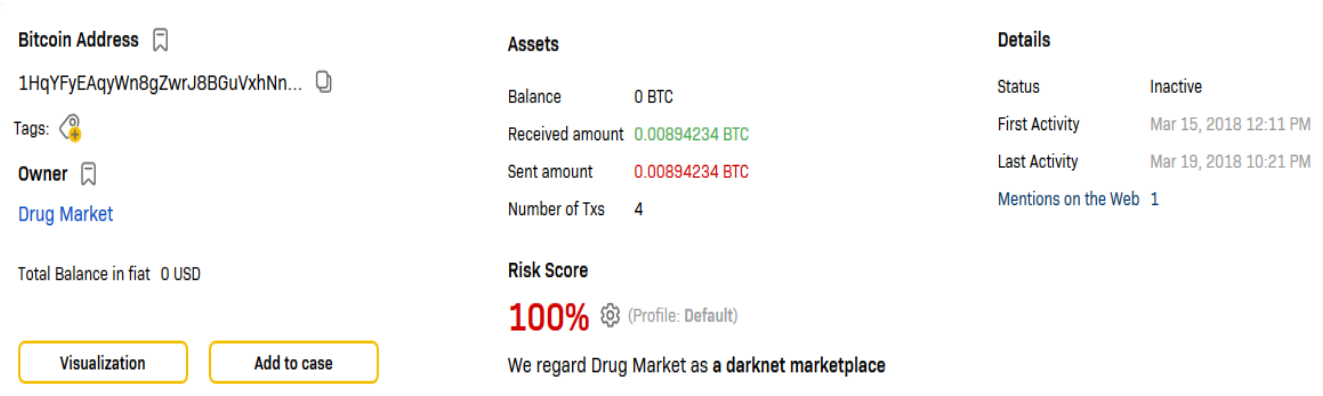


Мал. 16 – Фрагмент перевірки трансакції інструменту "Монітор (Monitor)"

Інструмент **"Інформаційна панель (Dashboard)"** розділений на 4 секції інформування користувача про створені і збережені ним:

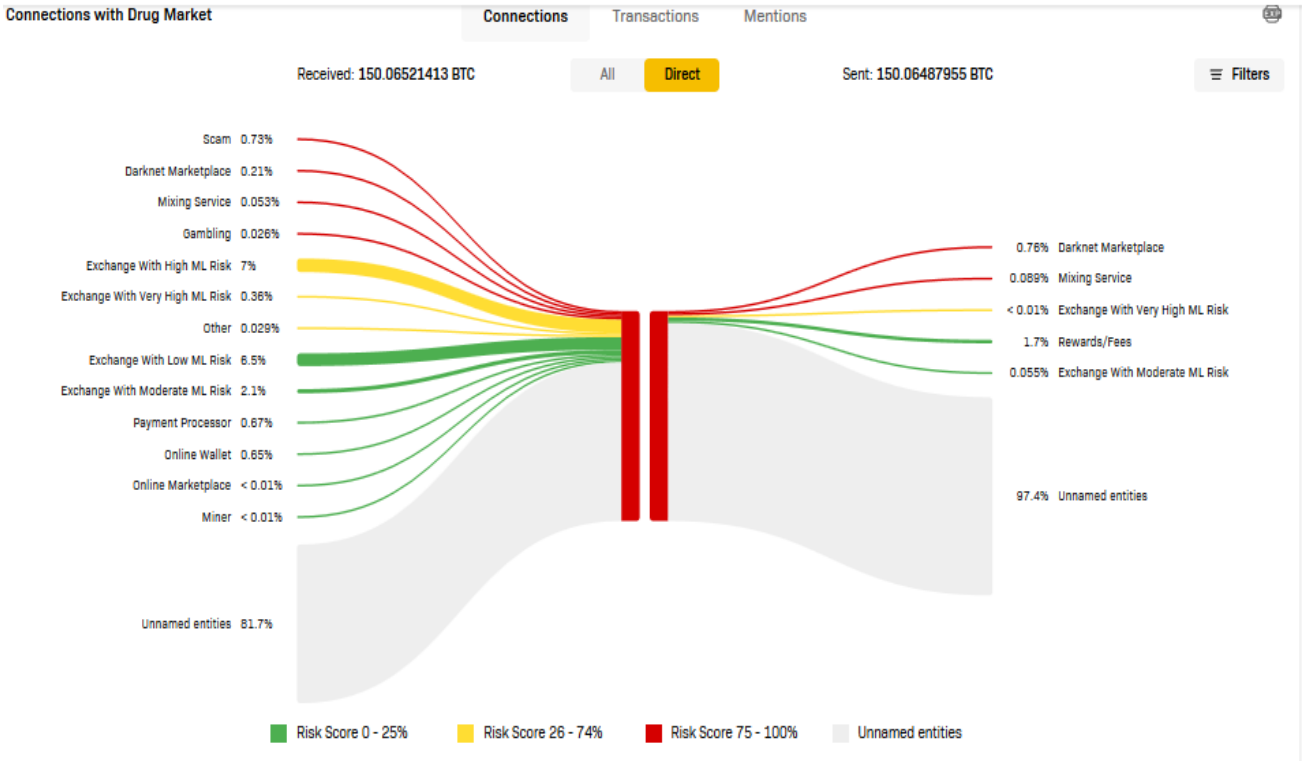
- Справи (Cases);
- Візуалізації (Visualizations);
- Закладки (Labeles) сторінок аналізу адрес, блоків трансакцій, трансакцій та володільців адрес;
- Перелік відстеження (Tracking List) руху коштів.

При дослідженні в основному інструменті "Дослідник (Explorer)" певної біткоїн-адреси Crystal надає інформацію про категорію володільця адреси, поточний баланс, кількість трансакцій, поточний стан, дати першої і останньої активності, величину ризику (Risk Score) щодо імовірної участі у кримінальній діяльності і кримінальності походження коштів (мал. 17).



Мал. 17 – Інформація про біткоїн-адресу

Тут же для володільця цієї адреси відображається загальна якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) з іншими ідентифікованими володільцями біткоїн-адрес із зазначенням величини ризику (мал. 18).



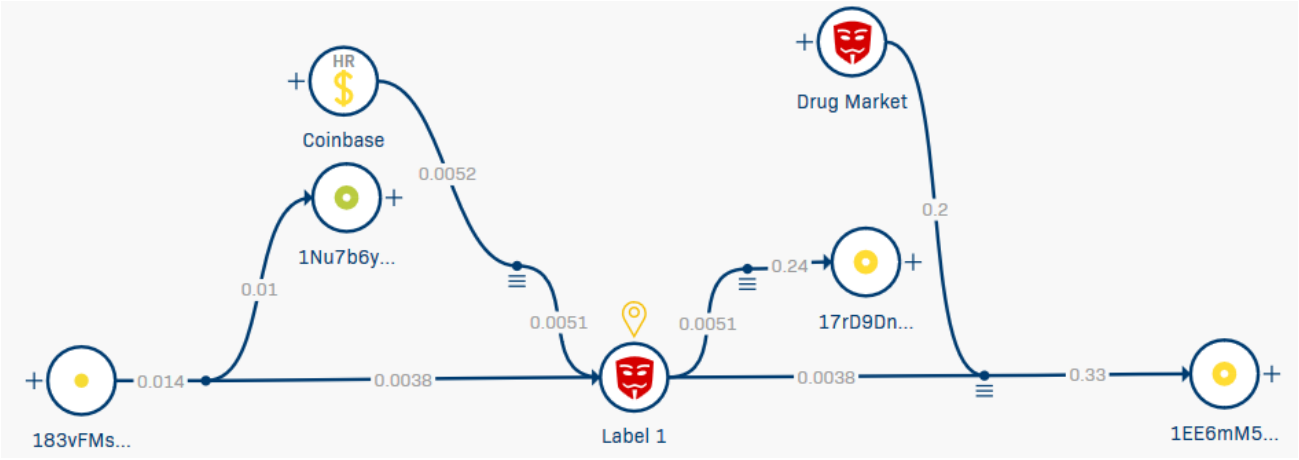
Мал. 18 – Якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) певної біткоїн-адреси з іншими ідентифікованими володільцями біткоїн-адрес

Також трансакції діаграми наводяться у вигляді переліку (мал. 19) і кожну можна дослідити детально.

ENTITY	TYPE	RECEIVED, BTC ↓	SENT, BTC ↓	TRANSACTIONS ↓	FIRST INTERACTION ↓	LAST INTERACTION ↓
273360557	Unnamed entities	20	0	1	Jun 21, 2017 02:54:42 am	Jun 21, 2017 02:54:42 am
Coinbase	Exchange With High ML Risk	9.07066636	0	470	Jan 31, 2017 07:08:25 pm	Dec 06, 2018 02:04:11 am
BitcoinDE	Exchange With Low ML Risk	4.20835526	0	72	Feb 02, 2017 06:02:52 pm	Dec 22, 2018 10:50:22 am
Paxful	Exchange With Moderate ML Risk	2.37246193	0	106	Feb 12, 2017 09:13:49 pm	Dec 14, 2018 04:22:02 pm

Мал. 19 – Фрагмент списку трансакцій володільця біткоїн-адреси, що досліджується

Через інструмент "Візуалізація (Visualization)" трансакції з біткоїн-адресом, що досліджується, можна представити у вигляді графа (мал. 20) та керувати відображенням вузлів графа.



Мал. 20 – Візуалізація трансакцій з біткоїн-адресом, що досліджується

З огляду на зазначений функціонал платформа Crystal Expert може ефективно забезпечувати розслідування кримінальних правопорушень, в яких фігурують визначені криптовалюти.

1.2 Типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, пов'язаних із незаконним обігом наркотиків та ін. із використанням сучасних телекомунікаційних та інших технологій.

Аналіз матеріалів слідчої та судової практики дозволяє виділити такі типові слідчі ситуації початкового етапу розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів із використанням сучасних телекомунікаційних та інших технологій:

Перша слідча ситуація. *Незаконний обіг наркотиків з використанням сучасних телекомунікаційних та інших технологій, наявні певні відомості про особу збувальника.* Зазначена ситуація виникає, як правило, при встановленні слідчим ознак незаконного розповсюдження наркотиків з використанням мережі Інтернет при розслідуванні іншого злочину у межах іншого кримінального провадження. Також ця ситуація формується при затриманні особи, яка незаконно переміщувала наркотичні засоби, психотропні речовини, їх аналоги чи (і) прекурсори, або особи, яка організувала та утримувала місце для вживання, виготовлення, виробництва наркотиків, коли затримані особи в

якості джерела походження вилучених наркотиків вказують їх придбання через мережу Інтернет.

Основні тактичні завдання у цій ситуації полягають у фіксації ознак вчиненого затриманими злочину та встановленні особи (осіб), які продали наркотики з використанням мережі Інтернет. Зазначені завдання можуть бути вирішені під час проведення слідчих (розшукових) дій, у тому числі негласних, та інших заходів, характерних для розслідування злочинів, пов'язаних із незаконним обігом наркотиків. Водночас слід відзначити притаманність цим діям певних особливостей, а також необхідність проводити певні не специфічні для розслідування незаконного обігу наркотиків слідчі (розшукові) дії, у т.ч. негласні, що обумовлені саме використаним злочинцями способом незаконного збуту наркотиків – з використанням сучасних телекомунікаційних та інших технологій. Зокрема, типовій слідчій (розшуковій) дії – допиту підозрюваного – будуть притаманні особливості, пов'язані із колом обставин, що підлягатимуть з'ясуванню. Наприклад, предмет допиту підозрюваних має бути розширений за рахунок встановлення ознак та обставин придбання ними наркотиків через мережу Інтернет, групу у месенджері, використаних для цього технічних пристроях і програмах, способах безготівкового розрахунку зі збувальниками тощо. З метою перевірки отриманих показань слідчому доцільно проводити огляд місця події, специфічність якого полягатиме у об'єкті огляду – Інтернет-сторінки, сайту чи сторінки у соціальній комп'ютерній мережі, групового чату у певному месенджері, що містять оголошення, рекламу, контактні дані збувальників, листування з приводу збуту наркотиків. Якщо в результаті допиту буде встановлено факт листування збувальника з покупцем каналами електронної пошти з використанням українського поштового сервісу, слід отримати ухвалу слідчого судді на здійснення тимчасового доступу до листування. Також слід відзначити й необхідність призначення комп'ютерно-технічної чи (і) телекомунікаційної експертизи щодо вилучених при затриманні та обшуку комп'ютерів, смартфонів, інших пристроїв, використаних підозрюваними для пошуку в мережі Інтернет інформації про збут наркотиків,

для встановлення зв'язку та спілкування зі збувальниками з приводу придбання наркотичних засобів, психотропних речовин та прекурсорів.

Друга слідча ситуація. *Має місце систематичний збут наркотиків з використанням сучасних телекомунікаційних та інших технологій, інформація про збувальника незначна або відсутня.* Зазначена слідча ситуація характерна для самостійного виявлення слідчим, детективом чи оперативними працівниками ознак збуту наркотиків, що здійснюється через мережу Інтернет чи із використанням інших сучасних телекомунікаційних технологій або перевірки отриманого від громадян повідомлення про виявлення ознак розповсюдження наркотиків даним способом.

Основні тактичні завдання у цій ситуації полягають у необхідності фіксації факту незаконного збуту наркотиків з використанням сучасних телекомунікаційних та інших технологій та встановленні конкретних осіб (збувальника і його співучасників), причетних до цього. Зазначені завдання можуть бути досягнуті шляхом проведення таких слідчих (розшукових) дій, як допит свідка (заявника), огляд місця події (Інтернет-сторінки, сторінки у соціальній комп'ютерній мережі та ін.), направлення доручення в порядку статті 40 КПК України працівникам оперативних підрозділів про проведення слідчих (розшукових) дій, у т.ч. негласних. З дотриманням кримінального процесуального законодавства слід також здійснити тимчасовий доступ до інформації про абонента, що міститься у Інтернет провайдера, щодо діапазону IP-адрес, з яких збувальник здійснював вихід у мережу. За номерами телефонів, посилання на які встановлено при огляді Інтернет-сторінки, доцільно отримати також й ухвалу слідчого судді на здійснення тимчасового доступу до інформації про абонента та деталізацію з'єднань, що міститься у оператора зв'язку, який обслуговує телефонний номер збувальника. Якщо проведеними діями встановлений факт створення спеціального сайту для незаконного збуту наркотиків з використанням мережі Інтернет, слід отримати ухвалу слідчого судді на здійснення тимчасового доступу до серверів, з яких сайту надаються послуги хостингу, з метою вилучення відповідної інформації. За результатами

проведення зазначених слідчих (розшукових) дій проводяться й інші. Зокрема, допити, обшуки, затримання підозрюваних, призначення експертиз тощо.

При документуванні спеціально-створеного для збуту наркотиків сайту слід: а) за допомогою Інтернет-сервісу «whois» встановити реєстратора доменного імені та хостингову компанію; б) надіслати запит до реєстратора доменного імені про надання анкетних даних, повідомлених про себе реєстрантом, номеру телефону, реквізитів електронної скриньки, IP-адрес, що були використані для реєстрації та входу до панелі управління доменним іменем, платіжних реквізитів, використаних для оплати реєстрації доменного імені; в) отримати ухвалу суду на здійснення тимчасового доступу до інформації, що міститься в хостинговій компанії, про особу-замовника послуг хостингу сайту, IP-адресу адміністрування сайту, платіжних реквізитів, використаних для оплати послуг хостингу; г) у разі, якщо послуги реєстрації доменного імені чи хостингу надавались іноземними компаніями, відповідну інформацію можливо отримати по каналах Національної цілодобової мережі контактних пунктів реагування на кіберзлочини.

1.3. Особливості тактики проведення окремих слідчих (розшукових) та інших дій у алгоритмі розслідування незаконного обігу наркотиків та ін. із використанням сучасних телекомунікаційних та інших технологій.

Огляд місця події може бути проведений: а) за місцем затримання причетних до незаконного обігу наркотиків осіб; б) у всесвітній мережі Інтернет (сторінка в соціальній комп'ютерній мережі або веб-сайт із наявною інформацією про збут певного виду наркотиків, контактними даними особи збувальника тощо); б) за місцем перебування підозрюваного під час виходу у мережу Інтернет для розміщення оголошень про продаж наркотиків, листування із покупцями, надсилання їм повідомлень про місце та ознаки «закладки», ін.

Особливістю огляду місця події, пов'язаною з його «віртуальним» розташуванням є те, що основним об'єктом огляду стає сторінка в соціальній

комп'ютерній мережі, веб-сайт із наявною інформацією про збут певних наркотиків, контактними даними особи збувальника, тощо. Під час такого огляду, окрім безпосередньої письмової фіксації наявної інформації (адреса Інтернет-сторінки, на якій розміщена реклама або пропозиція придбати наркотики, зміст розміщеної інформації, контактні телефони, інші суттєві відомості) шляхом її внесення до протоколу огляду місця події, слід також скопіювати інформацію за допомогою скриншотів (знімків екрану). Вказані скриншоти мають бути скопійовані на носії інформації (бажано, оптичні диски одноразового використання), один з яких виконуватиме роль архівного, а інший – резервного. В подальшому такі носії підписуються, упаковуються належним чином та долучаються до протоколу огляду в якості додатків, про що мають бути зроблені відповідні позначки, як у протоколі даної слідчої (розшукової) дій, так і у додатках до нього. Скриншоти також можуть бути роздруковані, а дані роздруківки завірені підписом слідчого і також долучені як додатки до протоколу огляду місця події.

Огляд зазначених об'єктів може бути здійснено і у порядку ч. 2 ст. 264 КПК України, зокрема – у рамках зняття інформації з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Це стає можливим тільки в ситуації, коли на момент виникнення необхідності у невідкладному огляді, відомості про вчинене кримінальне правопорушення внесені до ЄРДР і кримінальне провадження розпочато.

Огляд предметів, об'єктами якого стають засоби комп'ютерної техніки, банківські картки, телефонні-картки, що використовувались злочинцями при незаконному обігу наркотиків через Інтернет, а також наркотичні засоби, психотропні речовини, їх аналоги та прекурсорі. Огляд зазначених об'єктів може бути здійснений, як самостійна слідча (розшукова) дія, так і в рамках огляду місця події.

Запит до адміністрації ресурсу про надання інформації щодо: а) назви облікових записів, від імені яких розміщена реклама, оголошення, останні дати відвідування; б) персональні дані, номер телефону, електронну пошту, що повідомлені про себе особою-користувачем, що здійснила незаконний обіг наркотиків під час реєстрації в мережі Інтернету та ін.; в) IP-адрес, з яких зловмисником здійснювалась реєстрація облікових записів та доступ до них.

Організація тактичної операції з метою встановлення та затримання особи, яка збуває наркотики з використанням мережі Інтернет, у тому числі, шляхом оперативної закупівлі наркотиків. Особливістю даної операції є використання правоохоронцями комп'ютерів та мережі Інтернет для встановлення «зашифрованого» контакту, спілкування та розрахунків зі збувальником, із подальшим долученням до матеріалів кримінального провадження протоколів відповідних слідчих (розшукових) чи негласних слідчих (розшукових) дій, додатків до них у вигляді носіїв комп'ютерної інформації, носіїв із відео- чи (і) аудіо записами та ін., що стануть об'єктами відповідних експертних досліджень.

Так, у кримінальному провадженні про збут наркотичних засобів і психотропних речовин, здійснюваний злочинною організацією, під час досудового слідства було проведено 6 оперативних закупівель.[12]

Затримання підозрюваного. Під час затримання підозрюваного можуть бути вилучені мобільні телефони, пакети із наркотиками, гроші, отримані від незаконного наркобізнесу, у вигляді вітчизняної та іноземної валюти (USD, EUR, ін.), а також банківські картки.

Огляд предметів вилучених при затриманні підозрюваного, а також в ході обшуку, а також при інших слідчих (розшукових) діях. При огляді мобільних телефонів слід звертати увагу на текстові та інші повідомлення, за якими можуть бути встановлені інші факти участі затриманого у незаконному

[12] Справу організованої групи закладників наркотиків і психотропів, яка працювала через Інтернет-магазин, направлено до суду. Інформаційне Агенство Інтерфакс-Україна. 20.08.2019р. // URL: https://ua.interfax.com.ua/news/general/608065.html (дата звернення – 01.11.2020).

обігу наркотиків, вчиненому з використанням мережі Інтернет, його співучасники, покупці наркотиків, місця, час та інші обставини вчинення даного та інших кримінальних правопорушень, пов'язаних із незаконним виробництвом, виготовленням, придбанням, зберіганням, пересиланням чи збутом наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет.

Також може бути проведений ще один вид огляду – ***огляд тіла живої людини або освідування*** в порядку ст. 241 КПК України за участю судово-медичного експерта чи лікаря на предмет встановлення на тілі підозрюваного / затриманого слідів ін'єкцій та інших зовнішніх ознак вживання наркотиків, а також знаходження у стані наркотичного сп'яніння тощо.

Допит підозрюваного. Має бути спрямований як на з'ясування механізму вчинення незаконного обігу наркотиків, так і на використання комп'ютерів, інформаційних технологій, мережі Інтернет при підготовці та вчиненні даних кримінальних правопорушень.

Допит осіб, які незаконно придбавали наркотичні засоби, психотропні речовини, їх аналоги та прекурсори за допомогою сучасних телекомунікаційних та інших технологій, пов'язаний із необхідністю з'ясування обставин, обумовлених застосуванням даного специфічного способу збуту наркотиків. Зокрема, під час допиту покупців слід встановити відомості щодо: 1) джерел походження інформації про придбання наркотиків через мережу Інтернет, месенджери, соціальні сторінки тощо (від кого дізнався, хто надав електронну адресу, телефон, дані сайту); 2) місць, часу виходу в мережу Інтернет з метою ознайомлення з пропозиціями купівлі/продажу наркотику, використаних для цього технічних засобах та контактних даних (логін); 3) характеристики сайту / Інтернет-сторінки (назва чату, блогу, сайту, номер ICQ, адреса електронної пошти, URL-адреса), чату, каналу у месенджері; 4) обставин встановлення контакту зі збувальником та його контактних даних, а також кількості та способів спілкування з розповсюджувачем наркотиків; 5) адресатів та способів оплати за придбані наркотики (поповнення рахунку певного телефонного

номеру; надання секретного коду ваучера поповнення рахунку шляхом SMS-повідомлення; здійснення банківського переказу; переказу коштів з рахунку віртуальної банківської картки, криптовалютна трансакція, тощо); 7) часу, обставин, та способу отримання інформації про місце схованки наркотику (Інтернет-повідомлення, SMS- чи MMS-повідомлення, ін.); 8) інших осіб, які замовляли наркотики, використовуючи мережу Інтернет.

Допит осіб, які здійснювали розповсюдження наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів за допомогою мережі Інтернет чи з використанням інших телекомунікаційних технологій передбачає необхідність з'ясування: 1) організаторів та співучасників розповсюдження наркотиків через мережу Інтернет чи інші сучасні телекомунікаційні та інші технології; 2) характеристики схеми незаконного збуту наркотиків (створення сайту чи(і) використання існуючих Інтернет-ресурсів, месенджерів для розміщення реклами та пропозицій щодо продажу наркотиків (назва чату, блогу, сайту, каналу, номер «ICQ», електронної скриньки, URL-адреси); 3) обставин та умов придбання й налагодження комп'ютерного обладнання, програмного забезпечення і засобів комунікації, що використовувались у злочинних цілях; 4) обставин використання Інтернет (послугами якого Інтернет-провайдера користувався, яким було ім'я користувача, частота зміни контактних даних); 5) місць та часу виходу в мережу Інтернет з метою незаконного збуту наркотиків; 6) способи, час та інші обставини спілкування з покупцями наркотиків, використання з цією метою технічних засобів та Інтернет; 7) способів оплати, обраного виду грошових коштів чи інших видів розрахунків та способів перевірки їх надходження від конкретної особи (покупця); 8) способів передачі наркотиків покупцю; 9) шляхів отримання, конвертації, легалізації та використання коштів, отриманих від збуту наркотиків, ін.

Тимчасовий доступ до речей і документів. За даними виявлених банківських карток слід отримати від фінансових установ відомості про власників карткових рахунків, які брали участь у незаконному обігу наркотиків

та послуги яких використовувались для отримання коштів від збуту наркотиків з використанням мережі Інтернет, про рух коштів за цими рахунками, а також фотографій з банкоматів, зроблених при знятті готівки. Також за необхідності слід отримати відеозаписи камер зовнішнього відеоспостереження, прилеглих до банкоматів, де знімалась готівка. У подальшому за отриманими відомостями проводяться слідчі (розшукові) дії, у тому числі негласні, спрямовані на встановлення всіх осіб, причетних до незаконного обігу наркотиків з використанням мережі Інтернет, їх затримання та притягнення до кримінальної відповідальності.

Також слід отримати ухвалу слідчого судді про тимчасовий доступ до речей і документів з метою отримання від Інтернет-провайдерів інформації щодо користувачів Інтернет-сайтів та власників поштових скриньок, які брали чи могли брати участь у незаконному обігу наркотиків з використанням мережі Інтернет, а також окремо про огляд отриманої інформації та її носіїв.

Доручення в порядку статті 40 КПК України про проведення слідчих (розшукових) дій, у тому числі негласних, спрямованих на встановлення співучасників незаконного обігу наркотиків з використанням сучасних телекомунікаційних та інших технологій (у тому числі, які мешкають у інших населених пунктах) та їхнє затримання. За необхідності до таких доручень слід додавати відповідні ухвали суду.

Обшуки у кримінальних провадженнях за фактом збуту наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів з використанням сучасних телекомунікаційних та інших технологій проводяться за місцем проживання, роботи, зберігання майна підозрюваного, місцем здійснення незаконних операцій з наркотиками, ін.

Метою проведення зазначених обшуків є відшукання та вилучення:

а) наркотичних засобів, психотропних речовин, їх аналогів чи (і) прекурсорів, засобів та знарядь для їхнього виготовлення чи (і) виробництва, пакувальних матеріалів, чернеток із записами про покупців, обсяги торгівлі тощо);

б) комп’ютерного обладнання та телекомунікаційних засобів, що використовував підозрюваний у злочинних цілях (ЕОМ, інші засоби комунікації та комплектуючі деталі до них, цифрові модеми провідного та безпровідного Інтернет-зв’язку, засоби цифрового відео- та аудіо- зв’язку (веб-камери, мікрофони тощо), фото- відеотехніка (якщо повідомлення про місцезнаходження наркотиків надходило у відео- або фотографічному форматі, у оголошеннях про збут наркотиків, розміщених у Інтернет, містились фото та відео файли), термінали рухомого (мобільного) зв’язку – телефонні апарати (із зазначенням їх IMEI-номерів), картки поповнення рахунку операторів (провайдерів) телекомунікацій (Інтернет та мобільного зв’язку), телефонні SIM-картки операторів (провайдерів) телекомунікацій, використані пластикові пакування карток поповнення рахунку операторів (провайдерів) телекомунікацій та SIM-карток;

в) носіїв комп’ютерної інформації із відомостями про відвідування певних сайтів, створення і розміщення рекламних оголошень на певних Інтернет-сторінках, листування із конкретними особами з приводу незаконного обігу наркотиків, ін.;

г) предметів, документів та відомостей про отримання та використання грошових коштів від незаконного обігу наркотиків (паперові чеки банківських установ про отримання грошових коштів, договори з банком чи банківськими установами про відкриття банківського рахунку, установчі документи про відкриття підприємства, установи, організації, пластикові магнітні картки банківських установ, кошти, які були предметом оперативної закупівлі наркотиків, інші документи, які підтверджують здійснення грошових оборудок (накладні, розписки, чеки, декларації, договори тощо), а також кошти, цінності, інші предмети, які могли бути отримані в результаті вчинення протиправної діяльності.

Так, у кримінальному провадженні в ході обшуків за місцями проживання фігурантів виявлено та вилучено наркотичні засоби та психотропи у великих та особливо великих розмірах (героїн, амфетамін, «солі», канабіс тощо),

пристосування для їх вживання, ваги, пакувальний матеріал, банківські картки, гроші, а також системний блок, на якому фахівці кіберполіції виявили фотоматеріали із зображенням місць схованок наркотиків.[13]

Призначення судових експертиз:

1) *експертизи наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів*, яка дозволяє розпізнати й встановити належність досліджуваного об'єкту до наркотику, встановити присутність на предметі-носії слідів наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів, визначити кількісний вміст та можливість виготовлення з представлених речовин наркотичних засобів та психотропних речовин;

2) *судово-медичної експертизи підозрюваного* для встановлення наявності на його тілі тілесних ушкоджень, слідів ін'єкцій, часу та механізму їх виникнення, ступеня тяжкості тощо;

3) *дактилоскопічної експертизи* за відбитками пальців на упакуванні наркотиків, обладнанні для його виготовлення, портативних носіях інформації (флеш-пам'ять, оптичні диски), комп'ютерній техніці, смартфонах, банківських картках та інших предметах, виявлених під час огляду чи(і) обшуку з метою встановлення всіх співучасників незаконного обігу наркотиків;

4) *комп'ютерно-технічної експертизи* з метою встановлення наявності на носіях інформації, у засобах комунікації, комп'ютерах тощо певної інформації (наприклад, відомостей про відвідування певних сайтів, створення і розміщення рекламних оголошень на певних Інтернет сторінках, листування із конкретними особами з приводу незаконного обігу наркотиків, ін.), часу її утворення, наявності певного програмного забезпечення, що дозволило створити графічні, текстові, відео-файли із інформацією про продаж певних видів наркотиків, ін.;

5) *телекомунікаційної експертизи* (новий вид експертиз). На сьогодні єдиним дієвим способом пошуку слідів злочину вчиненого з використанням електронних платіжних систем, криптовалют, інших віртуальних коштів, та

[13] Справу організованої групи закладників наркотиків і психотропів, яка працювала через Інтернет-магазин, направлено до суду. Інформаційне Агенство Інтерфакс-Україна. 20.08.2019 р. // URL: https://ua.interfax.com.ua/news/general/608065.html

перетворення потенційної інформації що знаходиться в цих слідах злочину в доказову інформацію є проведення телекомунікаційної експертизи. Вона проводиться з метою вирішення таких питань: діагностичних – щодо виявлення властивостей і стану об'єктів, наданих на експертизу, як при їх безпосередньому вивченні, так і по їхньому відображенню; аналізу ситуації в цілому, коли після дослідження стану об'єктів чи їхніх відображень встановлюється їх взаємозв'язок, наявність зв'язку окремих явищ між собою і з подією злочину; ідентифікаційних для ототожнення конкретного телекомунікаційного засобу в мережі чи(і) конкретного користувача телекомунікаційного засобу; встановлення факту переведення коштів між електронними гаманцями (в тому числі криптовалютними, або інших віртуальних коштів); встановлення факту наявності коштів на конкретному електронному гаманці (в тому числі криптовалютному, або інших віртуальних коштів); з якого були проведенні зазначені операції з переміщення коштів з або на конкретний електронний гаманець (в тому числі криптовалютний, або інших віртуальних коштів); ідентифікації користувача конкретного телекомунікаційного засобу; визначення імовірного знаходження (географічного, за координатами) телекомунікаційного засобу в певний проміжок часу; трекінгу (відстеження маршруту) вже проведених та поточних почтових відправлень; фіксування та документування фактів створення та підтримання електронних ресурсів з незаконного розповсюдження наркотичних засобів; встановлення факту електронної переписки між злочинцями, або злочинцями та кінцевими споживачами наркотичних засобів (на форумах, за допомогою месенджерів, у соціальних комп'ютерних мережах, мобільним зв'язком та ін.);

6) *судової-наркологічної експертизи підозрюваного* з метою встановлення наркотичної залежності чи(і) *психіатричної експертизи* для вирішення питань його осудності (за необхідності);

7) *інших судових експертиз* за всіма вилученими об'єктами з метою з'ясування та доказування всіх обставин механізму вчинення злочинів, пов'язаних із незаконним обігом наркотиків, вчиненим через Інтернет.

Пошук та вилучення записів камер зовнішнього чи(і) внутрішнього відеоспостереження, у яких зафіксовано перебування підозрюваного у приміщеннях чи інших місцях, де він виходив у мережу Інтернет (Інтернет клуби, зони покриття Wi-Fi тощо), здійснював закладку наркотиків, отримував грошові кошти у банку чи(і) банкоматі тощо.

Допит в якості ***свідків*** осіб, яким відомі певні обставини вчиненого злочину. До таких осіб можуть бути віднесені особи, які: 1) виявили відомості про незаконний обіг наркотиків, наприклад, рекламу, оголошення на Інтернет-сайтах чи сторінках у соціальних мережах, адреси каналів, чатів у месенджерах тощо; 2) як співробітники Інтернет-кав'ярень надавали послуги доступу до Інтернет підозрюваним у незаконному обігу наркотиків; 3) виявили «закладки» з наркотиками та повідомили про це поліцію; 4) проживають неподалік місць виявлених «закладок» та бачили підозрілих осіб, які могли бути причетні до приховування наркотиків у цих місцях; 5) стали очевидцями затримання осіб, причетних до незаконного обігу наркотиків та ін. Відповідно, у ході допиту зазначених осіб слід максимально уточнити й деталізувати обставини, які вони безпосередньо спостерігали та які допоможуть встановити і довести причетність конкретних осіб до незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів з використанням сучасних телекомунікаційних та інших технологій. Також в якості свідків у кримінальних провадженнях про досліджувані злочини можуть бути допитані родичі, члени родини, друзі, знайомі підозрюваних, співробітники правоохоронних органів, споживачі наркотиків, інші особи.

Збір відомостей, що характеризують особу підозрюваного(них). Зважаючи на механізм незаконного обігу наркотиків з використанням мережі Інтернет, особливу увагу слід приділити виявленню документів чи інших джерел інформації про наявність у підозрюваного освіти у галузі комп'ютерних технологій, досвіду роботи у відповідній сфері, наявності відповідних практичних вмінь та навичок. В окремих випадках виникає потреба у вилученні й інших документів, що характеризують підозрюваного (наприклад, медичних

карток з медичних закладів, довідок про лікування, знаходження на обліку у нарколога, психіатра та ін.) з метою їх долучення до матеріалів кримінального провадження, використання при призначенні і проведенні певних судових експертиз тощо.

1.4. Правові основи та загальні принципи взаємодії працівників кіберполіції зі слідчим

Правова основа *регулювання питань взаємодії працівників підрозділів кіберполіції зі слідчим під час проведення досудового розслідування.*

На сьогодні досить важливо, щоб взаємодія в системі правоохоронної діяльності, зокрема між працівниками кіберполіції та слідчими здійснювалась відповідно до чинного законодавства України та міжвідомчих і відомчих нормативно-правових актів. Правовою основою взаємодії є Конституція України, Міжнародні правові акти, рішення Європейського суду з прав людини, національні закони і підзаконні акти, які умовно можна поділити на дві групи.

Перша група – це Конституція України, закони і підзаконні акти, якими визначаються організаційні основи взаємодії, завдання, функції та повноваження.

Друга група – міжвідомчі та відомчі нормативно-правові акти, зокрема накази, інструкції, положення, що регламентують права і обов'язки суб'єктів взаємодії, їх повноваження, функції, форми і методи спільної діяльності, а також регулюють порядок взаємодії, визначають конкретні напрями.

Першу групу, як правову основу взаємодії працівників кіберполіції із слідчим становлять:

1. Конституція України, Кримінальний та Кримінальний процесуальний кодекси України, Цивільний і Цивільний процесуальний кодекси України та ін.

2. Закони України: «Про Національну поліцію», «Про прокуратуру», «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» та ін.

3. Міжнародні правові акти, що ратифіковані Верховною Радою України та рішення Європейського суду з прав людини.

4. Підзаконні нормативні акти: накази, положення, постанови, що видаються МВС України, Національною поліцією України, Офісом Генерального прокурора, Службою безпеки України (СБУ), Міністерством юстиції України та ін. Значення підзаконних нормативних актів полягає у тому, що вони сприяють правильній реалізації законодавчих розпоряджень та в окремих випадках визначають механізм їх виконання.

При цьому, необхідно звернути увагу на те, що сьогодні правоохоронні органи України знаходяться в постійному стані кардинального реформування. У зв'язку з цим регулярно вносяться зміни як до чинного кримінального процесуального законодавства України, так і до відомчих нормативно-правових актів, що пов'язано з прийняттям і вступом у дію ряду нових Законів. Законодавча і нормативна-правова база, що безпосередньо регулює питання взаємодії органів досудового розслідування з оперативними підрозділами ґрунтується, в тому числі :

-*іншими законами :*

Законом України від 02. 2015 р. № 580-УШ «Про Національну поліцію» зі змінами станом на вересень 2020 р.;

Законом України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» зі змінами станом на вересень 2020 р.;

Законом України від 22 лютого 2000 року № 1489-Ш «Про психіатричну допомогу» зі змінами станом на вересень 2020 року.

У той же час на сьогодні більшу частину законів і нормативно-правових актів, які були прийняті відповідно до положень Закону України «Про міліцію» (*втратив чинність*), так і не приведено у відповідність до Закону України «Про Національну поліцію».

До основних міжнародно-правових актів у відповідному напрямі слід віднести, до першої групи: 1) Конвенцію Ради Європи «Про протидію злочинності у сфері комп'ютерної інформації ETS № 185» яка радифікована

Верховною Радою України із застереженнями і заявами Законом від 07.09. 2005 р. ВВР. 2006. №5-6. Ст. 71; 2) Рішення Європейського Суду з прав людини та ін.

Другу групу становлять нормативно-правові акти*, зокрема*:

1. Положення про органи досудового розслідування Національної поліції України та Інструкція з організації діяльності органів досудового розслідування Національної поліції України, які затверджені наказом МВС України від 06.07.2017 року. № 570.
2. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні», затвердженою наказом МВС України від 07.07. 2017 р. № 575.
3. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затвердженою спільним наказом Генеральної прокуратури України, МВС України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1687/5 від та інші.
4. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України, затвердженої наказом МВС України від 27. 04.2020 р. № 357.
5. Наказ МВС України від 18.05. 2020 р. № 393 «Про затвердження Змін до Інструкції з організації обліку та руху кримінальних проваджень в органах досудового розслідування Національної поліції України».
6. Інструкція про порядок використання правоохоронними органами України системи Міжнародної організації кримінальної поліції – Інтерпол, *затвердженої* спільним наказом МВС України, Офісом Генерального прокурора, Національним антикорупційним бюро України, Службою безпеки України, Державним бюро

розслідувань, Міністерством фінансів України, Міністерством юстиції України від 17.08.2020 р. № 613/380/93/228/414/510/2801/5.

7. Інструкція про порядок вилучення, обліку, зберігання та передачі речових доказів у кримінальних справах, цінностей та іншого майна органами дізнання, досудового слідства і суду від 27.08. 2010 р. за №51/401/649/471/23/125 в новій редакції станом на вересень 2020 р., затвердженої Генеральною прокуратурою України, МВС України, Державною податковою адміністрацією України, Службою безпеки України, Верховним судом України, Державною судовою адміністрацією України.

8. Іноді в ролі правових основ взаємодії органів досудового розслідування з іншими підрозділами можуть виступати та використовуватись також й постанови та Листи Пленуму Верховного Суду України та колишнього Вищого Спеціалізованого Суду України (які чинні й на сьогодні).

Відповідно до пункту 4 Прикінцевих та перехідних положень Закону України «Про Національну поліцію» до приведення законодавства України у відповідність із цим Законом акти законодавства застосовуються в частині, що не суперечить йому.

Тому, окремо та більш детально слід розглянути порядок взаємодії, що наближено до нашої тематики, який зокрема висвітлено в **«Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні»,** затвердженої наказом **від 07.07.2017 № 575.**

Відповідно, в ній зокрема, окремо закріплено наступні положення щодо особливостей організації взаємодії при досудовому розслідуванні кримінальних правопорушень **у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) :**

1. Досудове розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж

електрозв’язку здійснюється слідчими, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду.

2. Матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп’ютерів, систем та комп’ютерних мереж і мереж електрозв’язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити:

1) письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм), а також у разі наявності документи, що підтверджують право власності потерпілого на комп’ютерну інформацію та інформацію, що передається мережами електрозв’язку, чи програмно-технічні засоби;

2) установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі та мережі електрозв’язку (логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв’язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо).

3. Утворення СОГ за участю оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп`ютерів, систем та комп`ютерних мереж і мереж електрозв`язку здійснюється за спільним наказом керівників органу досудового розслідування та Департаменту кіберполіції Національної поліції України. Утворення СОГ у кримінальному провадженні, досудове розслідування у якому здійснюється Головним слідчим управлінням

Національної поліції України, здійснюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України – начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції Національної поліції України. Старшим СОГ є слідчий, якого керівником органу досудового розслідування визначено здійснювати досудове розслідування кримінального правопорушення.

4. Керівник Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, оперативний працівник якого включений до складу СОГ або за матеріалами якого розпочато кримінальне провадження, забезпечує взаємодію з органом досудового розслідування Національної поліції України, який здійснює розслідування кримінальних правопорушень зазначеної категорії.

З вказаних пунктів Інструкції про взаємодію між працівниками кіберполіції та слідчими можна зробити висновок, що працівники кіберполіції можуть бути залучені слідчим для надання практичної допомоги при розслідуванні вказаних специфічних видів злочинів. Зазвичай слідчим в порядку ст. 40 КПК України надається відповідне письмове доручення підрозділу кіберполіції для виконання певних слідчих (розшукових) дій чи надання роз'яснень з питань вчинених злочинах, пов'язаних з електронно обчислювальною технікою (по 9 статтях XVI розділу «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'терних мереж і мереж електрозв'язку» КК України). У той же час, треба брати до уваги, що слідчий частіше не може мати достатніх знань для формулювання правильних питань чи дій що доручено кіберполіцейським та вважає їх залучення можливим тільки в злочинах комп'ютерної сфери, що призводить до неякісних результатів виконання доручення та як наслідок неповного розслідування кримінального провадження. В практичному аспекті, працівники кіберполіції мають спеціальні знання не тільки в сфері високих технологій, а й в оперативно-

розшуковій діяльності, зокрема що може відігравати значну роль при розслідуванні будь-яких злочинів (шахрайств, крадіжок, порушень авторських прав чи розповсюдження незаконного контенту).

Для ефективної взаємодії слідчим необхідно постійно підтримувати зв'язок та корегувати спільні дії перед тим як делегувати повноваження і надавати доручення. З цією метою доцільним є створення СОГ, для розслідування злочинів, які можуть містити в собі декілька причетних осіб чи епізодів злочинної діяльності. На сьогоднішній день законодавчо не закріплено вичерпний перелік функцій і повноважень кіберполіції, але кіберполіцейські на разі беруть участь в слідчих (розшукових) діях у якості спеціалістів та оперативних працівників, зокрема при проведенні обшуків, спеціального слідчого експерименту, допиту чи огляду комп'ютерної чи іншої спеціальної техніки.

Поняття взаємодії підрозділів кіберполіції під час проведення досудового розслідування

Для подальшого сприйняття і використання необхідно визначити поняття «взаємодії», основними суб'єктами якої є слідчі та оперативні підрозділи. Вчений І.В. Кубарєв, проаналізувавши процесуальне законодавство, визначив авторське бачення взаємодії, що полягає в узгодженому визначенні та здійсненні слідчих дій, оперативно-розшукових та інших заходів під керівництвом слідчого з метою ефективного вирішення завдань кримінального судочинства.

В свою чергу, А. А. Патик, досліджуючи питання взаємодії оперативного працівника і слідчого, визначає більш широко поняття «взаємодії» – як узгоджені, такі що випливають із завдань кримінального судочинства, комплексні (процесуальні і оперативно-розшукові) дії, метою яких є викриття, розкриття, розслідування і запобігання злочинам, притягнення до відповідальності винних осіб, виключно на підставах, визначених нормами кримінального процесуального закону, нормативними актами, що здійснюється при суворому розмежуванні компетенції, у межах наданих

повноважень, шляхом найбільш ефективного сполучення дозволених їм заходів і матеріального забезпечення при збереженні таємниці досудового розслідування і джерел отримання конфіденційних відомостей.

Як свідчить практика, чітка та ефективна організація взаємодії різних підрозділів правоохоронних органів під час проведення досудового розслідування безпосередньо спрямована на вирішення завдань кримінального провадження (ст. 2 КПК України). Особливої уваги дане питання набуває у зв'язку із продовженням радикального і концептуального реформування правоохоронних органів та прийняттям чинного КПК України у 2012 р., а також Законів України «Про прокуратуру», «Про Національну поліцію» та нормативно-правових актів, що регламентують діяльність суб'єктів, які залучаються до проведення досудового розслідування. Зазначене обумовлено наступними чинниками:

- **по-перше**, необхідністю досягнення злагодженої роботи співробітників кіберполіції та слідчих правоохоронних органів при вирішенні конкретних практичних питань, що виникають під час досудового розслідування кримінальних правопорушень;
- **по-друге**, дефіцитом часу, що стає негативним фактором під час проведення досудового розслідування, оскільки воно обмежено конкретними строками, зокрема дотримання розумних строків і строків досудового розслідування. Так, відповідно до ст. 28 КПК України, під час кримінального провадження кожна процесуальна дія або процесуальне рішення повинні бути виконані або прийняті в розумні строки. Розумними вважаються строки, що є об'єктивно необхідними для виконання процесуальних дій та прийняття процесуальних рішень. Розумні строки не можуть перевищувати передбачені КПК України строки виконання окремих процесуальних дій або прийняття окремих процесуальних рішень. Проведення досудового розслідування у розумні строки забезпечує прокурор, слідчий суддя (в частині строків розгляду питань, віднесених до його компетенції), а судового провадження – суд.

Критеріями для визначення розумності строків кримінального провадження є:

1) складність кримінального провадження, яка визначається з урахуванням кількості підозрюваних, обвинувачуваних та кримінальних правопорушень, щодо яких здійснюється провадження, обсягу та специфіки процесуальних дій, необхідних для здійснення досудового розслідування тощо;

2) поведінка учасників кримінального провадження;

3) спосіб здійснення слідчим, прокурором і судом своїх повноважень.

Відповідно до положень ст. 219 чинного КПК України досудове розслідування повинно бути закінчено:

1) протягом одного місяця з дня повідомлення особі про підозру у вчиненні кримінального проступку;

2) протягом двох місяців з дня повідомлення особі про підозру у вчиненні злочину.

Тому, саме за допомогою злагодженої співпраці різних органів і підрозділів, які залучаються до сфери кримінального процесу, процесуальна діяльність буде своєчасною та ефективною.

Слід зазначити, що відповідно до частини 3 ст. 13 Закону України «Про Національну поліцію» у складі поліції функціонують:

1) кримінальна поліція;

2) патрульна поліція;

3) органи досудового розслідування;

4) поліція охорони;

5) спеціальна поліція;

6) поліція особливого призначення.

Варто звернути увагу на те, що сьогодні спостерігається активізація багатостороннього співробітництва правоохоронних та інших компетентних органів у різних формах взаємодії. Однак у ході практичної реалізації поставлених завдань вони зіштовхуються з наявністю певних проблемних питань, що стосуються правового, організаційного, криміналістичного, матеріального, технічного, кадрового забезпечення. Отже, якість взаємодії органів і підрозділів під час досудового розслідування значною мірою

залежить від наділення учасників взаємодії відповідними правами та обов'язками.

Водночас на сьогодні кримінальне процесуальне законодавство України не містить чіткого визначення поняття «взаємодія», у зв'язку з чим залишаються не врегульовані права та обов'язки учасників процесу взаємодії. На відомчому рівні порядок взаємодії органів досудового розслідування з іншими органами та підрозділами закріплено в «Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні», затвердженої Наказом **МВС України від 07.07. 2017 № 575.**

Під організацією взаємодії органів і підрозділів під час проведення досудового розслідування слід розуміти узгоджену співпрацю осіб, залучених до кримінальних процесуальних правовідносин, діяльність яких регламентується законами та іншими відомчими нормативно-правовими актами, і яка необхідна для досягнення завдань конкретного кримінального провадження, а також спрямована на обговорення отриманих результатів і планування подальших заходів.

Отже, в цілому можна зазначити, що значення взаємодії органів під час досудового розслідування полягає у забезпеченні цілеспрямованих та ефективних заходів, спрямованих на швидке, повне та неупереджене розслідування та вирішення справи по суті.

Завдання, принципи та напрями взаємодії підрозділів під час проведення досудового розслідування.

Основним завданням взаємодії органів та підрозділів під час проведення досудового розслідування є запобігання, попередження, виявлення і розслідування кримінальних правопорушень, притягнення до встановленої законодавством відповідальності осіб, що їх вчинили, відшкодування завданої кримінальними правопорушеннями шкоди, відновлення порушених прав та законних інтересів фізичних і юридичних осіб.

Основними принципами взаємодії, які в юридичній літературі іноді називаються *умовами*, є:

1. Відповідальність слідчого за швидке, повне та неупереджене розслідування кримінальних правопорушень, його самостійність у процесуальній діяльності, втручання в яку осіб, що не мають на те законних повноважень, забороняється. Слідчий несе відповідальність за законність та своєчасність здійснення процесуальних дій (ст. 40 КПК України).

2. Активне використання методик, наукових і технічних досягнень у попередженні, виявленні та розслідуванні кримінальних правопорушень.

3. Оптимальне використання наявних можливостей слідчих і оперативних підрозділів у попередженні, виявленні та розслідуванні кримінальних правопорушень.

4. Дотримання загальних засад кримінального провадження (Глава 2 КПК України). До них відносяться:

- *Законність*. Принцип законності є одним із основних і проходить через діяльність правоохоронних органів. Даний принцип є основою для реалізації інших принципів у кримінальному судочинстві. Під час взаємодії законність передбачає чітке дотримання приписів закону при здійсненні процесуальних дій. Це правило поширюється на дотримання порядку взаємодії, а також на відповідне процесуальне оформлення її результатів;

– *Відповідність спільної діяльності вимогам закону.* Реалізація даного принципу в процесі взаємодії виражається в точному і неухильному дотриманні слідчими й оперативними підрозділами всіх законів і підзаконних нормативних актів, що регулюють їх спільну погоджену діяльність.

5. Забезпечення нерозголошення даних досудового розслідування. Зокрема, відповідно до ст. 222 КПК України відомості досудового розслідування можна розголошувати лише з дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим. У необхідних випадках слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв’язку з участю в ньому, про їх обов’язок не розголошувати такі відомості

без його дозволу. Незаконне розголошення відомостей досудового розслідування тягне за собою кримінальну відповідальність, встановлену законом.

Також до ***принципів*** взаємодії підрозділів під час проведення досудового розслідування слід віднести наступні:

– системність;

– плановість;

– розподіл компетенції.

Тобто, спільне планування слідчих і оперативно-розшукових заходів це найважливіша організуюча основа будь-якої усвідомленої людської діяльності, необхідна передумова її ефективності. План слідчих та оперативно-розшукових заходів повинен бути спільним. Це пов’язано з тим, що, по-перше, метою спільного планування є найбільш ефективне використання всіх засобів, які є у слідчого, по-друге, наявність спільного плану, затвердженого керівником органу досудового розслідування, дозволяє персоніфікувати відповідальність за якість та строки виконання тих чи інших заходів.

Необхідно звернути увагу на те, що в ході взаємодії повинно бути враховано безперервність в такому виді організаторської роботи, тому що, ефективність спільної діяльності значною мірою залежить від тривалості взаємодії та міри об’єднання зусиль.

Як зазначалося вище, взаємодія на практиці організується залежно від конкретних ситуацій, які виникають під час розслідування того чи іншого кримінального провадження. У ході вирішення таких ситуацій між слідчим та оперативними підрозділами виникають різноманітні зв’язки та взаємовідносини. Конкретні способи та порядок цих зв’язків виражається в певних формах, що існують поряд із принципами взаємодії.

В цілому взаємодія здійснюється за *двома напрямами*:

1. **Стратегічному** – організація реалізації державної політики у протидії злочинності, усуненні причин і умов її існування, а також удосконалення законодавчої та нормативно-правової бази.

2. **Тактичному** – виявленні, документуванні й припиненні кримінальних правопорушень, попередженні, розкритті та розслідуванні вчинених кримінальних правопорушень, розшуці і затриманні підозрюваних осіб, а також відшкодуванні шкоди фізичним та юридичним особам.

Також необхідно пам'ятати, що взаємодія здійснюється на двох рівнях:

1) на центральному рівні – між Головним управлінням органів і підрозділів, які залучаються до проведення досудового розслідування (наприклад, Головного слідчого управління Національної поліції та Генеральної прокуратури України); Між підрозділами ГСУ і Управлінням дізнання Національної поліції;

2) на регіональному рівні – між головними управліннями, а також управліннями в Автономній Республіці Крим, областях, містах Києві та Севастополі.

Основні види та форми взаємодії працівників кіберполіції зі слідством

У юридичній літературі, окрім визначення поняття «взаємодія» також немає чіткого обґрунтування та розподілу видів і форм взаємодії, але більшість учених-процесуалістів вважають, що існує їх розподіл на процесуальні та організаційні (не процесуальні).

До *процесуальних форм* взаємодії відносяться:

1. Письмові доручення слідчого, дізнавача, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, які є обов'язковими для виконання оперативним підрозділом (ст. 41 КПК України). Термін виконання доручень не повинен перевищувати встановленого у них строку. У разі неможливості своєчасного виконання доручення продовження строку його виконання письмово погоджується начальником оперативного підрозділу з керівником

слідчого підрозділу (дізнання) **(згідно п. 6.6 «Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції у попередженні, виявленні та розслідуванні кримінальних правопорушень»** затвердженої наказом МВС України **від 07.07. 2017 р. № 575).**

2. Надання допомоги слідчому (дізнавачу) при провадженні окремих слідчих (розшукових) дій (разове доручення). Допомога оперативних підрозділів необхідна слідчому (дізнавачу) при провадженні таких слідчих (розшукових) дій, які потребують великого обсягу роботи або додаткових гарантій для осіб, котрі беруть у них участь. Це огляди місця події, обшуки, слідчі експерименти та ін. Участь співробітника оперативного підрозділу відображається в протоколі слідчої дії.

До *організаційних форм (не процесуальних)* взаємодії працівників оперативних підрозділів і слідчого (дізнавач), тобто тих, що передбачені відомчими нормативними актами, відносяться:

1) *сумісне та погоджене планування,* яке полягає в складанні погодженого плану слідчих (розшукових) дій та негласних слідчих (розшукових) дій;

2) с*умісне провадження слідчих (розшукових) дій та негласних слідчих (розшукових) дій.* На підставі інформації, яка відома, слідчий та співробітник оперативного підрозділу спільно висувають та перевіряють всі версії. Висунуті в процесі обговорення версії повинні знайти своє відображення як у плані розслідування, в якому вказуються всі необхідні для перевірки версії слідчих (розшукових) дій, так і у плані оперативно-розшукових дій, який складають оперативні працівники. У планах також потрібно визначити завдання, які слід вирішити на першочерговому етапі розслідування, намітити слідчі (розшукові) дії, за допомогою яких планується їх вирішення, узгодити організаційні питання по проведенню всіх дій (час виконання, виконавці, зв’язок і взаємна інформація);

3) *спільна погоджена діяльність у складі слідчо-оперативної групи (СОГ)* – наступний спосіб здійснення ефективного розслідування для забезпечення принципу об’єктивності;

4) *обмін інформацією та спільне обговорення результатів слідчих (розшукових) дій та негласних слідчих (розшукових) дій.* У ході проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій спільне обговорення та складання плану може мати місце декілька разів, залежно від отримання нової інформації та ситуації, яка склалася в ході розслідування. При цьому, слідчий (дізнавач) та співробітник оперативного підрозділу повинні постійно дотримуватись такої обов’язкової умови, як взаємний обмін інформацією, в тому числі і оперативно-розшуковою. Спільне вивчення (аналіз і оцінка) матеріалів, отриманих у процесі розслідування, дозволяє підійти до них з різних позицій, точніше визначити напрями подальшої діяльності слідчого (дізнавача) й співробітника оперативного підрозділу, обставини, що потрібно виявити.

Взаємний обмін інформацією між співробітником оперативного підрозділу і слідчим (дізнавачем) – необхідна умова взаємодії. Зміст взаємодії полягає у наданні один одному інформації, отриманої в процесі оперативно-розшукової діяльності та слідчих (розшукових) діях, які становлять спільний інтерес та завдання розслідування конкретного кримінального правопорушення.

5) *консультації* між слідчими (дізнавачем) та оперативними працівниками, які готують і проводять слідчі (розшукові) і негласні слідчі (розшукові) дії в межах кримінального провадження;

6) *спільний аналіз* причин і умов, що сприяють вчиненню кримінальних правопорушень та обговорення профілактичних заходів.

7) *спільне використання техніки, засобів зв'язку і транспорту*, що має в своєму розпорядженні оперативні підрозділи тощо.

Слід мати на увазі, що таке розмежування форм – умовне, тому що процесуальні форми взаємодії знаходять більш детальне регламентування у

відомчих нормативних актах, а організаційні – або оговорені, але недостатньо повно визначені та регламентовані законом, або випливають з його змісту.

В залежності від періоду часу, протягом якого здійснюється взаємодія і від ступеня об'єднання спільних зусиль, можна виділити такі її *види*:

а) разова;

б) періодична;

в) постійно діюча.

Координацію діяльності оперативних підрозділів і досудового розслідування по виявленню і розслідуванню кримінальних правопорушень здійснюють керівники відомств у межах свого відомства, а прокурор – всіх органів досудового розслідування. Тому однією з головних форм взаємодії на стадії досудового розслідування є проведення спільних нарад і колегій міністерств і відомств, які взаємодіють у розгляді найактуальніших проблем, що виникають у процесі виявлення та розслідування кримінальних правопорушень, прийняття узгоджених рішень щодо реалізації завдань кримінального провадження.

Організація взаємодії при створенні слідчо-оперативних груп при проведенні досудового розслідування про кіберзлочини.

Для виконання завдань кримінального провадження (ст. 2 КПК України) щодо швидкого, повного та неупередженого розслідування кіберзлочинів можуть утворюватися слідчо-оперативні групи (далі – СОГ).

Утворення СОГ здійснюється за *наказом начальника територіального органу поліції, погодженого з керівником слідчого підрозділу*. При цьому керівником СОГ є слідчий, який визначений керівником слідчого підрозділу здійснювати досудове розслідування кримінального правопорушення. До складу СОГ, як правило, включаються співробітники, які брали участь в огляді місця події. У разі потреби залучаються дільничні інспектори поліції, на території обслуговування яких учинено кримінальне правопорушення, співробітники інших органів та підрозділів поліції. За для більш повної узгодженості у діях, керівник слідчо-оперативної групи складає погоджений

план дій з вказівкою на робочі версії за даним кримінальним правопорушенням та заходами, що направленні на його розкриття, при цьому вказуються як оперативно-розшукові заходи так і слідчі (розшукові) дії, а також зазначаються виконавці та строки виконання цих заходів й дій. Забороняється здійснювати заміну співробітників оперативних підрозділів, що включені до складу слідчо-оперативної групи, без узгодження зі слідчим (керівником групи) або керівником органу досудового розслідування.

Контроль за роботою СОГ покладається на керівника слідчого підрозділу, який за погодженням з начальником територіального органу поліції вправі організовувати проведення оперативних нарад за участю слідчих та працівників інших органів і підрозділів поліції з питань виявлення, розкриття та розслідування кримінальних правопорушень, у тому числі стану виконання доручень слідчих та взаємодії служб.

Для організації розслідування кіберзлочинів, вчинених у минулі роки, наказом начальника територіального органу поліції, погодженого з керівником слідчого підрозділу створюються **спеціалізовані постійно діючі СОГ.**

Для досудового розслідування кримінальних правопорушень, вчинених *на території декількох районів регіону*, наказом начальника ГУНП, УНП, погодженим з начальником слідчого управління (відділу) ГУНП, УМНП, може створюватися **СОГ ГУНП, УНП.** Контроль за її роботою покладається на слідче управління (відділ) ГУНП, УНП.

Для досудового розслідування кримінальних правопорушень, вчинених на території декількох областей (регіонів), наказом центральним органом Національної поліції може створюватися **міжрегіональна СОГ.** Контроль за її роботою покладається на Головне слідче управління Національної поліції або слідче управління (відділ) ГУНП, УНП, на території обслуговування якого вчинено найбільшу кількість кримінальних правопорушень.

Питання взаємодії при виконанні письмових доручень слідчого (дізнавача)

Необхідно звернути увагу на те, що *співробітники оперативних підрозділів* **не мають права** *здійснювати процесуальні дії* в кримінальному провадженні *за власною ініціативою або звертатися з клопотанням по цих питаннях* до слідчого судді чи прокурора.

Під час досудового розслідування кримінальних правопорушень *слідчий надає* відповідним оперативним підрозділам поліції, а в разі створення СОГ – конкретним співробітникам оперативного підрозділу, включеним до її складу, *письмові доручення про проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій* (далі – доручення). Дізнавач дає доручення уповноваженим оперативним підрозділам поліції під час досудового розслідування кримінальних проступків.

Необхідність розгляду питання виконання співробітником оперативного підрозділу письмових доручень слідчого (дізнавача) про проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій обумовлено його прикладним характером. Так, у практичній діяльності з боку працівників оперативних підрозділів можна почути нарікання з приводу того, що слідчі в окремих випадках «зловживають» своїми повноваженнями і доручають виконання таких дій, які вони могли б виконати самостійно. При цьому виконання доручень слідчого оперативним підрозділом мають вигляд формальної відповіді, про що свідчать наявні в матеріалах досудового розслідування відповіді, які в більшості випадків будується на конструкції словосполучення: *«не виявилось / не представилось можливим…» та ін.*

Відповідно до ч. 3 ст. 41 КПК України **доручення слідчого, дізнача** щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій **є обов'язковими для виконання оперативним підрозділом**, який під час їх виконання користується його повноваженнями. *Співробітники оперативних підрозділів не мають права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою* або звертатися з клопотанням до слідчого судді чи прокурора щодо надання їм можливості їх виконати.

В дорученні щодо провадження слідчих (розшукових) та негласних слідчих (розшукових) дій оперативним підрозділом *слідчий, дізнавач повинен чітко формулювати для виконавця його мету*. Від неї залежить наявність або відсутність в дорученні відповідних рекомендацій щодо виконання розшукового завдання. Крім цього, *у доручені повинно бути зазначено найменування кримінального провадження та його реєстраційний номер; короткий виклад фактичних обставин кримінального правопорушення; перелік слідчих (розшукових) дій чи негласних слідчих (розшукових) дій, які потрібно виконати; інші відомості, які необхідні для виконання цих дій*. Відзначимо, що відповідно до ст. 300 КПК України дізнавач має право виконувати негласні слідчі (розшукові) дії, передбачені ч. 2 ст. 264 та ст. 268 КПК України.

Слід відмітити, що чинним КПК України *не визначено строки виконання процесуальних дій за дорученнями* слідчого, дізнавача, прокурора. Окремі положення КПК України містять вказівки на строки проведення процесуальних дій, але не вказують їх терміни. Зокрема, *ч. 8 ст. 223 КПК України* наголошує, що «*слідчі (розшукові) дії не можуть проводитися після закінчення строків досудового розслідування*», які визначені положеннями ст. 219 КПК України. Разом з тим окремі питання виконання оперативним працівником доручень також урегульовано «*Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні», затвердженої Наказом МВС України від 07.07.2017 року № 575*. Зокрема в ній передбачено, що **письмові доручення слідчих, дізнавачів** щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) **є обов'язковими для виконання оперативним підрозділом**, а *термін їх виконання не повинен перевищувати встановленого у них строку*. Тобто, для виконання слідчих (розшукових) дій та негласних слідчих (розшукових) *слідчий, дізнавач може самостійно*, виходячи з обставин кримінального провадження встановити

певний строк і вимагати від співробітника оперативного підрозділу повідомлення про результати їх виконання. У зв'язку з чим слідчий, дізнавач в дорученні повинен зазначати: *«доручення підлягає виконанню у найкоротший строк, який не повинен перевищувати* (*вказати необхідний строк виконання*)». У разі *неможливості своєчасного виконання доручення продовження строку його виконання письмово погоджується начальником оперативного підрозділу з керівником слідчого підрозділу та керівником органу дізнання*.

Доручення, які надаються оперативному підрозділу, повинні бути *зареєстрованими в канцелярії* територіального органу поліції та передавитися в порядку, передбаченому «Інструкцією про організацію діловодства в системі МВС України», затвердженою Наказом МВС України від 23.08.2012 року № 747.

Матеріали про виконання доручень слідчих, дізнавачів *направляються* до слідчого підрозділу чи підрозділу дізнання *разом із супровідним листом за підписом начальника територіального органу поліції, який реєструється в канцелярії цього органу*.

Контроль за виконанням співробітниками оперативних підрозділів доручень слідчих, дізнавачів покладається на начальника територіального органу поліції, який зобов'язаний визначати конкретну особу або осіб, з числа співробітників оперативних підрозділів, на яких буде покладений обов'язок із виконання доручення слідчого (за виключенням доручень, які надаються співробітникам оперативного підрозділу, включеним до складу СОГ).

Слід визначити ще й інший напрям взаємодії, що здійснюється з *міжнародними правоохоронними* та іншими інституціями, як за участю співробітників оперативних підрозділів, зокрема кіберполіції, так і слідчих. Так, розділом IX чинного КПК України «Міжнародне співробітництво під час кримінального провадження», зокрема його 73-ма статтями регулюються

вказаний напрям оперативно-розшукової та слідчої діяльності в розрізі питань, що виникають у правозастосовній діяльності.

Крім цього, окремо слід визначити цілі та форми взаємодії у **міжнародному співробітництві** з використанням інформаційної **системи Інтерполу,** що регулюється «**Інструкцією про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол»,** *затвердженої* спільним наказом МВС України, Офісом Генерального прокурора, Національним антикорупційним бюро України, Службою безпеки України, Державним бюро розслідувань, Міністерством фінансів України, Міністерством юстиції України **від 17.08.2020 р. № 613/380/93/228/414/510/2801/5.**

Основні напрями наступні **:**

1. Міжнародне співробітництво правоохоронних органів України з органами Інтерполу, НЦБ іноземних держав, компетентними органами іноземних держав та міжнародними установами з використанням інформаційної системи Інтерполу здійснюється з питань та у формах, визначених правилами Інтерполу.

2. Цілями міжнародного співробітництва з використанням інформаційної системи Інтерполу є:

- установлення місцезнаходження осіб, які розшукуються, з метою їх затримання, арешту, обмеження свободи пересування та подальшої видачі (екстрадиції);

- установлення місцезнаходження осіб чи об'єктів, що становлять інтерес для правоохоронних органів України чи інших держав-членів Інтерполу;

- надання чи отримання інформації, що стосується розслідування злочинів, кримінального минулого або злочинної діяльності осіб;

- надання чи отримання інформації з метою попередження про осіб, події, об'єкти, способи вчинення злочинів, що становлять реальну загрозу публічній безпеці та порядку й можуть завдати істотної шкоди майну чи громадянам;

- ідентифікація осіб чи невпізнаних трупів;

- проведення криміналістичних досліджень;

- надання чи отримання інформації з питань публічної безпеки і порядку;

- ідентифікація загроз, організованих груп та злочинних організацій, тенденцій розвитку злочинності;

- обмін досвідом з питань боротьби із злочинністю та правоохоронної діяльності.

3. Обробка інформації в інформаційній системі Інтерполу здійснюється виключно для досягнення визначених Інструкцією (зазначена вище) цілей міжнародного співробітництва.

4. Використання інформаційної системи Інтерполу правоохоронними органами України здійснюється відповідно до встановленого Інструкцією (зазначена вище) порядку у формі надсилання запиту/звернення до уповноваженого підрозділу або у формі прямого доступу.

5. Уповноважений підрозділ на підставі отриманого від правоохоронного органу України запиту/звернення забезпечує використання інформаційної системи Інтерполу шляхом:

1) надсилання запиту про публікацію Генеральним секретаріатом Інтерполу оповіщень:

Червоного оповіщення (RED NOTICE);

Синього оповіщення (BLUE NOTICE);

Зеленого оповіщення (GREENNOTICE);

Жовтого оповіщення (YELLOW NOTICE);

Чорного оповіщення (BLACK NOTICE);

Пурпурного оповіщення (PURPLE NOTICE);

Помаранчевого оповіщення (ORANGE NOTICE);

Оповіщення про викрадені культурні цінності;

2) надсилання циркулярного оповіщення (циркуляра);

3) надсилання повідомлення;

4) внесення інформації до банків даних Інтерполу, її коригування або видалення;

5) отримання інформації з банків даних Інтерполу.

Крім того, уповноважений підрозділ надсилає до органів Інтерполу, НЦБ іноземних держав, компетентних органів іноземних держав та міжнародних установ запити, документи або інформацію відповідно до міжнародних договорів України у випадках, в яких передбачається використання каналів зв'язку Інтерполу.

6. Порядок оформлення та надсилання повідомлень, циркулярних оповіщень (циркулярів), запитів про публікацію Генеральним секретаріатом Інтерполу оповіщень, а також внесення інформації до банків даних Інтерполу, її коригування або видалення та отримання інформації з банків даних Інтерполу визначається цією Інструкцією та правилами Інтерполу.

7. Інформаційна система Інтерполу використовується для обміну відомостями про фізичних та юридичних осіб, об'єкти, події та факти лише в рамках відповідного кримінального провадження та/або оперативно-розшукової (розшукової) справи (за умови вжиття вичерпних заходів на національному рівні), а також заходів з питань публічної безпеки і порядку, запобігання перетинанню та недопущення перетинання державного кордону України особами, яким заборонено в'їзд або обмежено виїзд з України.

8. Інформація, отримана з використанням інформаційної системи Інтерполу, призначена виключно для використання правоохоронними органами України та судами для запобігання злочинам, виявлення, припинення, розкриття та розслідування злочинів, забезпечення публічної безпеки і порядку, підтримання публічного обвинувачення та судового провадження, здійснення ідентифікації особи у випадках, передбачених законодавством.

9. Правоохоронні органи України зобов'язані забезпечити ефективний захист інформації, яку отримують та передають з використанням інформаційної системи Інтерполу (міжвідомчий наказ від 17.08.2020 №613/380/93/228/414/510/2801/5.

Відомості, що обробляються в інформаційній системі Інтерполу, можуть передаватися засобам масової інформації лише з дозволу тих органів Інтерполу, НЦБ іноземних держав, компетентних органів іноземних держав, міжнародних установ, правоохоронних органів України, які надали їх для обробки і в тому обсязі, в якому вони визнають можливим.

Організація взаємодії працівників кіберполіції зі слідчим на початковому етапі досудового розслідування

Організація взаємодії при надходженні заяв і повідомлень про кіберзлочини

При надходженні до органу поліції заяви або повідомлення про вчинене кримінальне правопорушення оперативний черговий територіального органу поліції (далі – оперативний черговий) зобов'язаний негайно надати її начальнику слідчого підрозділу, який визначає слідчого, що здійснюватиме досудове розслідування, а також поінформувати начальника територіального органу поліції.

Слідчий невідкладно, але не пізніше 24 годин зобов'язаний внести відомості про кримінальне правопорушення за заявою,повідомленням або рапортом оперативного працівника до Єдиного реєстру досудових розслідувань (далі – ЄРДР).

Начальник територіального органу поліції повинен організувати своєчасне направлення на місце події слідчо-оперативну групу (далі – СОГ) у повному складі.

Слідчо-оперативні групи створюються при чергових частинах територіальних органів поліції. Склад цих груп формується з працівників органу поліції відповідно до графіку чергування, затвердженого начальником територіального органу поліції та погодженого з начальником слідчого підрозділу. До СОГ в обов'язковому порядку входять слідчий (старший СОГ), співробітник оперативного підрозділу та інспектор-криміналіст. *Потрібно зауважити*, що на тепер відповідно до «Інструкції про порядок залучення працівників органів досудового розслідування поліції та

Експертної служби Міністерства внутрішніх справ України, затвердженої Наказом МВС України від 03.11.2015 року № 1339 залучається *не спеціаліст-криміналіст (скасовано), а* ***інспектор-криміналіст***. **Завданням СОГ є виявлення, фіксація, кваліфіковане вилучення та пакування слідів кримінального правопорушення, речових доказів, встановлення свідків та потерпілих, з'ясування обставин кримінального правопорушення, що мають значення для всебічного, повного і неупередженого їх дослідження та встановлення осіб, причетних до його вчинення**.

Після прибуття на місце події члени СОГ з'ясовують обставини вчинення кримінального правопорушення, встановлюють свідків, прикмети осіб, які вчинили кримінальне правопорушення та ймовірні шляхи їх відходу. У разі необхідності вживають заходів для переслідування транспортних засобів, якими заволоділи особи, що вчинили кримінальне правопорушення, або тих, що використовувалися при його вчиненні. Беруть участь у розшуку та затриманні осіб, які підозрюються в учиненні цих кримінальних правопорушень.

Слідчий, як керівник групи:

– керує діями членів СОГ та несе персональну відповідальність за якість проведення огляду місця події;

– разом з членами групи, залученими спеціалістами, запрошеними потерпілим, свідками та іншими учасниками кримінального провадження проводить огляд місця події, у ході якого в установленому КПК України порядку фіксує відомості щодо обставин учинення кримінального правопорушення, вилучає речі і документи, які мають значення для кримінального провадження, та речі, вилучені з обігу, у тому числі матеріальні об'єкти, придатні для з'ясування обставин, що підлягають доказуванню. Забезпечує їх належне зберігання для подальшого направлення для проведення експертного дослідження. Має право заборонити будь-якій особі залишати місце огляду до його закінчення та вчинювати будь-які дії, що заважають проведенню огляду;

– за наявності підстав інформує оперативного чергового про залучення додаткових сил і засобів для документування всіх обставин учиненого кримінального правопорушення;

– при необхідності допитує про обставини вчиненого кримінального правопорушення заявника, потерпілого, свідків та інших учасників кримінального провадження. Надає письмові доручення співробітникам оперативних підрозділів про проведення слідчих (розшукових) та негласних слідчих (розшукових) дій. Здійснює інші повноваження, передбачені КПК України.

***Співробітник оперативного підрозділу*:**

– здійснює збирання відомостей, що можуть бути використані як докази;

– установлює час, місце і обставини вчинення кримінального правопорушення; кількість причетних до його вчинення осіб, їх прикмети; наявність у них зброї, транспортних засобів, слідів на одязі чи тілі, які могли залишитися через опір потерпілих або при подоланні перешкод; індивідуальні ознаки викрадених речей; напрямок, в якому вони зникли, інші відомості, необхідні для встановлення осіб, які вчинили кримінальне правопорушення;

– негайно інформує слідчого, дізнавача про одержані дані щодо обставин вчинення кримінального правопорушення та причетних до нього осіб, для їх подальшої фіксації шляхом проведення слідчих (розшукових) та негласних слідчих (розшукових) дій;

– виконує письмові доручення слідчого, дізнавача про проведення слідчих (розшукових) та негласних слідчих (розшукових) дій. Під час їх виконання користується повноваженнями слідчого, дізнавача.

Інспектор-криміналіст *(спеціаліст-криміналіст)*:

– надає консультації слідчому з питань, що потребують відповідних спеціальних знань і навичок;

– з використанням спеціальних знань та навичок, науково-технічних засобів і спеціального обладнання проводить вимірювання, фотографування,

звуко- чи відеозапис, складає плани і схеми, виготовляє графічні зображення оглянутого місця чи окремих речей;

– виявляє, фіксує, здійснює вилучення та пакування матеріальних об'єктів, які несуть на собі слідову інформацію вчиненого правопорушення;

– проводить експрес-аналіз за зовнішніми характеристиками вилучених об'єктів (без надання письмового висновку), звертає увагу слідчого на фактичні дані, що мають значення для розслідування обставин кримінального правопорушення;

– несе персональну відповідальність за якісну фіксацію всієї слідової інформації, повноту відображених даних у протоколі огляду та схемі (плані) до нього.

У разі вчинення тяжких, особливо тяжких, а також кримінальних правопорушень, що викликають значний суспільний резонанс, огляд місця події проводиться за участю начальника територіального органу поліції та керівника слідчого підрозділу.

Крім цього, *якщо співробітником оперативного підрозділу отримана інформація про вчинене кримінальне правопорушення або яке готується, то він повинен зібрати матеріали перевірки за цим фактом, скласти рапорт та передати ці матеріали до чергової частини. Після передачі ним до чергової частини зібраних матеріалів (лише тих, які не мають грифу секретності) з відповідним рапортом про виявлення злочину оперативний черговий зобов'язаний негайно*:

1) зареєструвати в журналі єдиного обліку заяв і повідомлень про вчинені кримінальні правопорушення та інші події рапорт оперативного працівника про виявлення ним даного виду кримінального правопорушення;

2) надати вказані матеріали керівнику слідчого підрозділу;

3) проінформувати начальника територіального органу поліції про виявлення факту вчинення кримінального правопорушення.

Начальник слідчого підрозділу після отримання матеріалів перевірки визначає слідчого, який буде здійснювати досудове розслідування за фактом

вчинення кримінального правопорушення та відповідно до положень ст. 214 КПК України повинен розпочати досудове розслідування у кримінальному провадженні та зареєструвати цю інформацію у ЄРДР.

1.5. Використання можливостей соціальних мереж Інтернету при проведенні слідчих (розшукових) дій, негласних слідчих (розшукових) дій та оперативно-розшукових заходів

Починаючи з 2004 року широкого розповсюдження набули такі Інтернет – ресурси, як соціальні мережі. Кожен день сотні мільйонів людей спілкуються, знайомляться, обмінюються інформацією, фотографіями та відеозаписами, і навіть займаються комерційною діяльністю через різноманітні соціальні мережі, що нерідко залишається поза контролем податкової адміністрації та інших правоохоронних органів. Взірцем сучасних соціальних мереж звичайного вигляду та найбільш розповсюдженою мережею у світі (та поки що безкоштовною) є соціальна мережа, розроблена у 2004 року в США Марком Цукербергом, яка має відому та пізнавану назву «Facebook» [11]. Сам Марк Цукерберг за створення цієї соціальної мережі, у 2010 році був визнаний Американським журналом «Times» людиною року та став за її використання наймолодшим мільярдером. На пострадянському просторі, найвідомішими та поширеними у користуванні, навіть серед недостатньо обізнаних осіб щодо повних технічних можливостей мережі Інтернет, соціальними мережами також є «Facebook» та «Instagram». Обидві соціальні мережі, як «Facebook», так і «Instagram», на даний момент по своїм функціональним можливостям та структурі істотно відрізняються від інших соціальних мереж. Головний принцип, на якому ґрунтуються та використовуються майже усі існуючи соціальні мережі це добровільне створення користувачами своїх профілів та добровільне заповнення цих профілів інформацією про свою особистість. Зокрема, це інформація про особу користувача: місце, дату, місяць та рік його народження, місце проживання, навчальні заклади, в яких навчався чи навчається користувач, відомості про його родичів, відомості про соціальний та сімейний стан; вподобання користувача, зокрема: улюблені книги, кінофільми,

пісні, цитати відомих людей та інше; контактні дані користувача: номера телефонів, адрес електронної пошти, ім’я користувача в сервісі Telegram, номер сервісу Viber, адрес персонального Інтернет – сайту; особисті графічні та аудіо матеріали: фотографії та відеозаписи, на яких є сам користувач, або його родичі чи знайомі, цифрові зображення картин чи інші цифрові зображення, аудіо композиції, відеокліпи та відеоролики, котрі відображають, у тому числі естетичні або незвичайні смаки користувача. Всі ці дані користувачі соціальних мереж розміщують у своїх профілях добровільно, а не малозначним є те, що чим більше інформації про себе користувач розмістить в своєму профілі соціальної мережі, тим більший соціальний статус своєму профілю користувач здобуде за рахунок спілкування в мережі Інтернет. Тобто соціальні мережі стимулюють розміщення користувачами їх особистої інформації всередині самих соціальних мереж. Велика кількість людей, які мають створені в соціальних мережах профілі, тим самим відкривають для працівників правоохоронних органів вільний шлях для отримання інформації про певну особу.

Авторами науково-методичних рекомендацій проведено анкетування користувачів соціальної мережі «Facebook». Було проведено опитування 140 респондентів віком від 16 до 35 років, за результатами чого було отримано такі результати :

-70 % опитаних відвідують свою сторінку соціальної мережі «Facebook» щодня;

-80 % опитаних відкрили доступ до перегляду даних зі своєї сторінки соціальної мережі «Facebook» усім бажаючим;

-60 % опитаних використовують свою сторінку соціальної мережі «Facebook» для підтримання зв’язків з друзями;

-74 % опитаних розміщують на своїй сторінці соціальної мережі «Facebook» особисті дані, які повністю відповідають дійсності;

-70 % опитаних добавляють людей у список своїх друзів на своїй сторінці соціальної мережі «Facebook», спираючись на знайомство, чи на близькі дружні відносини з ними.

У той же час, лише 30 % опитаних не обмінюються і не планують обмінюватись на своїй сторінці соціальної мережі «Facebook» інформацією про вчинення протиправних діянь, шляхом використання повідомлень, хоча останні 70% таку можливість не виключають при спілкуванні через Інтернет.

Виходячи із наведених даних, необхідно наголосити, що використовуючи фотографії користувачів, які вони розміщують у своїх профілях соціальних мереж, таких як наприклад «Facebook та «Instagram», можливо дуже швидко та суттєво розширити та поповнити бази даних автоматизованих біометричних та інших систем, якими користуються працівники МВС та Національної поліції України відносно осіб що готують, вчиняють замах або вже вчинили кримінальне правопорушення чи ухиляються від досудового розслідування і суду. А це, в свою чергу, надасть і розширить працівникам правоохоронних органів наступні можливості:

- маючи фотографію чи фоторобот правопорушника – швидко ідентифікувати його особу у тому випадку, якщо його фотографії є в базі даних автоматизованої біометричної чи іншої системи;

- використати фотографії із списку «друзів» в сторінці соціальної мережі правопорушника з метою пред'явлення їх для впізнання потерпілому або свідкам кримінального правопорушення, а також для впізнання самого потерпілого в разі його вбивства чи смерті;

- наявність в базах даних автоматизованих біометричних систем багатьох фотографій однієї особи, але знятих з різних кутів та ракурсів дозволить ідентифікувати особу краще, якісніше й ефективніше, ніж використати звичайні обліки фотографій МВС, що зменшить чи унеможливить судову помилку;

- під час проведення оперативно-розшукового заходу дозволить більш повно та швидко встановити коло контактів і зв'язків особи;

- вказаний перелік не обмежує й інші можливості.

- можливо ідентифікувати особу за нік неймом та знаходити пов’язані аккаунти;

- пошук за фотографією схожої особи і відмітки інших осіб.

1.6. Методика фіксації слідів злочинного спрямування у мережі Інтернет, огляд структури файлової системи персонального комп’ютера

На базі використання системи класифікації способів вчинення кримінальних правопорушень у сфері сучасних інформаційних технологій, працівниками Інтерполу було розроблено кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачена класифікація комп’ютерних злочинів. В Європі, ще у 2001 році було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, яка більш відома в Україні під умовною на звою «Конвенція про кіберзлочинність». Крім того, Європейським комітетом з проблем злочинності Ради Європи у 1990 році, з метою визначення в Європі злочинів, пов'язаних із використанням сучасних комп'ютерних та інформаційних технологій, були підготовлені рекомендації про включення в законодавство європейських країн кримінальних норм «Мінімального списку» і «необов'язкового списку» щодо комп'ютерних злочинів. Всі зазначені закони, конвенції та підзаконні акти містять в собі визначення та класифікацію різноманітних злочинів у сфері комп’ютерної інформації. Але треба зазначити, що найбільшою проблемою в сфері розслідування злочинів вчинених у мережі Інтернет є виявлення та фіксації слідів злочинного спрямування. Це пов’язано з тим, що у разі, коли злочинець вчиняє протиправні дії на окремо взятому комп’ютері потерпілої особи чи використовує для цього свій комп’ютер, то навіть після видалення з комп’ютера даних злочинного спрямування, працівник правоохоронного органу все одно може ці данні знайти, відновити та вилучити в якості доказів. Інша річ, коли сліди злочинного спрямування знаходяться в мережі Інтернет.

Це може бути листування між злочинцями, чи листування між злочинцем і потерпілою особою. Також це можуть бути матеріали ксенофобного, чи

порнографічного характеру. У разі, якщо злочинець видалить інформацію злочинного спрямування з Інтернет ресурсу, то в таких випадках вже виникають проблеми збереження інформації, яка цікавить працівників правоохоронних органів, адже комп'ютер, на якому фізично була розміщена інформація злочинного спрямування може знаходитись, наприклад в Новій Зеландії, і вилучити його для проведення експертизи буде дуже не просто, а в більшості випадків навіть неможливо. На сьогоднішній день в Україні склалася така практика фіксації слідчим слідів злочинного спрямування в мережі Інтернет, як виготовлення у присутності понятих електронного знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет ресурс зі слідами злочинного спрямування, після чого дане зображення роздруковується, та приєднується до інших матеріалів кримінального провадження, а самі сторінки Інтернет ресурсу зберігаються на жорсткий диск, а потім записуються на CDR чи DVDR диск. Але у разі видалення інформації злочинного характеру зі сторінок Інтернет ресурсу, описаний вище електронний знімок втрачає свою процесуальну силу. Для того, щоб спростити процедуру виготовлення електронного знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет ресурс зі слідами злочинного спрямування, і використати його, як один із видів доказу під час кримінального провадження, ми пропонуємо створити програмне забезпечення для функціонування автоматизованої комп'ютерної системи, робота якої повинна ґрунтуватися на певних принципах, та мати в собі інформаційні блоки. Зокрема:

1) автоматизована комп'ютерна система повинна мати блок взаємодії з Єдиним державним реєстром досудового розслідування, чи повинна мати вигляд блоку розширення функцій зазначеного ЄДРДР. Тобто вхід до такої системи працівником правоохоронного органу повинен бути здійснений з використанням кодів доступу слідчих до ЄДРДР; 2) автоматизована комп'ютерна система повинна мати автоматизований блок виготовлення електронного знімку (так званий «print screen») будь якої частини чи сторінки

Інтернет ресурсу, а також автоматизований блок збереження усієї інформації, що знаходиться у будь-якій частині чи сторінці Інтернет ресурсу. За таких умов працівнику правоохоронного органу необхідно лише ввести в дану систему посилання на той чи інший Інтернет ресурс, на якому є інформація злочинного спрямування, а автоматизована комп'ютерна система вже без участі людини зробить вище зазначені дії з таким Інтернет ресурсом;

3) виготовлений електронний знімок (так званий «print screen»), а також вся збережена інформація з будь якої частини чи сторінки Інтернет ресурсу (а це може бути текст, графічна, аудіо та відео інформація), повинні зберігатись у вигляді окремих розділів бази даних, які повинні маркуватись із зазначенням: дати створення розділу бази даних; номеру кримінального провадження; посади працівника правоохоронного органу, який створив даний розділ; справжньої назви та електронного адресу Інтернет ресурсу, чи його частини, з якого зроблено електронний знімок та копія інформації країни та міста, де фізично знаходиться комп'ютер, на якому було розміщено Інтернет ресурс з інформацією злочинного спрямування, чи з інформацією, яка є слідами злочину.

Можна зробити висновок, що для реалізації вирішення зазначених проблем, щодо створення програмного забезпечення для функціонування автоматизованої комп'ютерної системи, необхідно провести відповідні дослідження, результати яких запровадити у практичну діяльність новостворених при ГУМВСУМВС України підрозділів боротьби з торгівлею наркотиками та кіберзлочинністю.

Факторами та чинниками, які суттєво ускладнюють можливість фіксації працівником поліції цифрової інформації, є: можливість у адміністратора Інтернет ресурсу (чи власника, що нерідко є синонімом) оперативно в управлінському розумінні змінювати його зміст, чи повністю його видалити з серверу; наявність можливості розташування серверів на території інших держав, та зокрема, на території тих держав, які не підписали міжнародні угоди щодо протидії кіберзлочинності; використання зловмисниками анонімних

програмних пакетів. Як зазначає Д. М. Цехан, «особливої гостроти ця проблема набуває у зв'язку з тим, що встановлення факту такого порушення є чи не найбільш значимою складовою процесу доказування у відповідних провадженнях».

Нижче ми приводимо декілька основних способів фіксації працівником поліції цифрової інформації, яка знаходиться в мережі Інтернет та представляє тактичний чи оперативний інтерес:

1) складання (друк) та подання відповідного рапорту працівником поліції;

2) відповідь провайдера, чи адміністрації Інтернет хостінгу на запит щодо змісту певного Інтернет сайту;

3) огляд в присутності понятих та друк тієї сторінки Інтернет ресурсу, яка представляє тактичний чи оперативний інтерес, через засоби WEB браузеру (комбінація клавіш «CTRL+P» чи вибір поля головного меню «Печать» або «Print»). Складання відповідного протоколу огляду;

4) огляд в присутності спеціаліста та друк тієї сторінки Інтернет ресурсу, яка представляє оперативний інтерес, через засоби WEBб раузеру (комбінація клавіш «CTRL+P» чи вибір поля головного меню «Печать» або «Print»). Складання відповідного протоколу огляду;

5) огляд в присутності понятих Інтернет ресурсу, який представляє оперативний інтерес. Виготовлення електронного знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет ресурс та його збереження. Збереження самого Інтернет ресурсу, який представляє тактичний чи оперативний інтерес, на жорсткий диск комп'ютера працівника поліції. Далі здійснюється друк виготовлених електронних знімків екрану та приєднання їх до інших матеріалів кримінального провадження. Запис на CDR чи DVDR диск, виготовлених електронних знімків екрану, та збережених під час огляду на жорсткий диск сторінок Інтернет ресурсу, що представляє тактичний чи оперативний інтерес. Після цього складається відповідний протокол щодо усіх виконаних дій.

1.7. Методика огляду структури файлової системи персонального компьютера захищеного паролем

Під час проведення працівниками поліції тимчасового доступу до речей і документів, обшуків чи оглядів місця події на підприємствах, установах, організаціях або у приватних осіб, може виникнути необхідність перевірити структуру файлової системи персонального комп'ютера (далі – ПК), чи серверу на предмет неліцензійного програмного забезпечення або інформації, яка представляє для слідчого тактичний чи для оперативного працівника оперативний інтерес.

В ході проведення зазначених дій, як правило, працівники поліції проводять їх без увімкнення комп'ютера та вилучають опечатують лише системний блок (персональний комп'ютер без монітору, колонок, маніпулятору «миша» та клавіатури), чи жорсткий диск, а після проведення зазначених процесуальних дій призначають проведення комп'ютерно-технічної експертизи. Але для більш надійної фіксації слідів злочину та швидкого використання при виявленні, розкритті та розслідуванні кримінального правопорушення доцільним є при проведенні названих дій увімкнення персонального комп'ютера та здійснення огляду його файлової системи в присутності понятих, внесення до протоколу огляду даних про версію та серійний номер встановленої на комп'ютері операційної системи, назви та характеристики внутрішніх пристроїв комп'ютеру, а також зазначення шляхів до папок, чи окремих файлів, що розташовані на жорсткому диску персонального комп'ютера чи серверу що оглядається. У практичній діяльності, коли працівники поліції будуть мати тимчасовий доступ до персонального комп'ютера чи сервера, в ході чого він буде вилучений і по наявній інформації будуть призначені експертизи, то в деяких випадках висновок експерта може надійти у термін понад одного місяця. В цей же період у працівників поліції можуть виникнути питання про наявність чи відсутність такої інформації на жорсткому диску для подальшої роботи у кримінальному провадженні. Таким чином, при виявленні неліцензійного програмного забезпечення чи інформації, яка представляє тактичний чи оперативний інтерес

на персональному комп’ютері чи сервері, файлова система яких оглядається, та після фіксації місцезнаходження зазначеної інформації у протоколі огляду – працівники правоохоронних органів отримують додаткові підстави для тимчасового доступу і вилучення персонального комп’ютера чи серверу та додаткову можливість поставити експерту більш конкретні запитання.

Але проблемність даних процесуальних і суто технічних дій полягає у тому, що у більшості випадків на вхід до операційної системи персональних комп’ютерів та серверів встановлено пароль і власник персонального комп’ютера чи серверу може відмовитися надати пароль для входу. Крім того, оскільки попередній огляд персонального комп’ютера чи серверу проводиться в присутності понятих, огляд доцільно проводити саме в тій операційній системі, що проінстальована на персональний комп’ютер чи сервері та під ім’ям кожного користувача, якщо їх декілька, а не взагалі зробити загальний огляд файлової системи. Це необхідно для того, щоб наглядно показати й роз’яснити понятим, що за операційна система встановлена на персональному комп’ютері чи сервері, скільки користувачів зареєстровано в даній операційній системі, яке програмне забезпечення встановлено у кожного з цих користувачів, та яка інформація зберігається в особистих розділах цих користувачів.

Окремо слід зазначити, що у будь-кому випадку включати під час огляду персональний комп'ютер, не знаючи заздалегідь пароль для входу в операційну систему є ризикованим кроком, тому, що існує багато видів програмного забезпечення, яке може просто видалити всі файли на жорсткому диску у разі, якщо було введено невірний пароль. І таким програмним забезпеченням правопорушники користуються не рідко. Саме тому й працівники поліції, в свою чергу, намагаються здійснити тимчасовий доступ до комп'ютера без його вмикання, що є логічним, але позбавляє можливості швидко отримати інформацію, яка може представляти для них тактичний чи оперативний інтерес.

На підставі викладеного при тимчасовому доступі до комп’ютера чи сервера можна рекомендувати два алгоритми огляду або вилучення системного блоку персонального комп’ютера чи сервера: перший – вилучення без увімкнення комп’ютера і другий – вилучення з увімкненням комп’ютера та оглядом структури його файлової системи.

При тимчасовому доступі до комп’ютера чи сервера і проведенні огляду і їх вилучення без його увімкнення, доцільним буде провести такі дії: в присутності понятих провести фотографування (або здійснити відеозйомку) системного блоку з усіх боків, обережно від'єднати від системного блоку усі сторонні пристрої та кабелі, провести зовнішній огляд системного блоку та окремо крупним планом сфотографувати чи зняти на відео наявні на ньому роз'єми та наклейки, після чого обклеїти усі бокові панелі системного блоку папером з відтисками печатки «для пакетів» того підрозділу поліції, що проводить тимчасовий доступ до комп’ютера чи сервера і здійснює огляд чи вилучення. Обклеювання папером з відтисками печатки бокових панелей системного блоку необхідно провести для того, щоб не санкціоноване відкриття панелей, в подальшому, без пошкодження паперу з відбитками печатки було б не можливо, і таким чином було б гарантовано збереження інформації на жорсткому диску комп'ютера до проведення комп'ютерно-технічної експертизи. Після цього системний блок персонального комп’ютера чи сервера необхідно помістити в ящик, мішок чи полімерний пакет, який необхідно прошити ниткою, обклеїти нитку та ящик, мішок чи пакет пояснювальною запискою, із зазначенням місця та часу огляду чи вилучення, вказати конкретно, що саме вилучається та упаковується, а також інформацію про понятих та особу, яка проводить вказані дії, після чого пояснювальна записка повинна бути підписана всіма учасниками.

Тимчасовий доступ до комп’ютера чи серверу та огляд їх з увімкненням комп’ютера та оглядом структури його файлової системи проводиться декількома способами, але після закінчення огляду структури файлової системи, системний блок персонального комп’ютера чи сервера необхідно оглянути та провести його вилучення так само, як і у випадку без включення комп’ютера. Не зважаючи на те, який саме алгоритм огляду комп’ютера при його увімкненні буде використаний, необхідно звернути увагу на те, що особі, яка отримала тимчасовий доступ до комп’ютера чи сервера і проводить огляд, необхідно буде спочатку загрузитись не з жорсткого диску комп’ютеру, а з CD чи DVD диску, або через підключений USB пристрій. Для цього працівнику поліції, який проводить огляд комп’ютеру, необхідно мати доступ до базової

системи вводу – виводу (англійською мовою – це широко відома абревіатура «BIOS») комп’ютеру, який може мати пароль для користування. Зазвичай, пароль в BIOS стирають таким чином: в присутності понятих відкривають системний блок, виймають батарейку з материнської плати, знаходять замкнуті контакти (зазвичай їх три) на материнській платі з підписом «cmos », або «clear cmos», або «clr cmos», або «clr_cm», перемикають замикач контактів (сленгова назва «джампер») на протилежні контакти (тобто, якщо було замкнено перший та другий контакти, то замикач контактів перемикають на другий та третій контакти), після чого вмикають комп’ютер, який може увімкнутись та не виводити жодної інформації на монітор, або комп’ютер може взагалі не увімкнутись. Далі, хоча б через п’ять хвилин після того, як було вилучено батарейку, цю саму батарейку необхідно поставити на своє місце, та ще раз увімкнути комп’ютер, який знову таким може увімкнутись та не виводити жодної інформації на монітор, або може взагалі не увімкнутись. Після цього, замикач контактів переставляють у те положення, в якому він був на момент відкриття системного блоку, вставляють батарейку на своє місце, закривають системний блок, та вмикають комп’ютер. У переважній більшості випадків, після зазначених дій з комп’ютером, пароль BIOS буде стертий. Але крім самого паролю, в BIOS також будуть стерті усі настройки роботи пристроїв комп’ютеру, а самий факт розбирання комп’ютера та фізичне втручання в роботу його електронної, а не програмної частини працівником поліції – є негативним фактором для збору і отримання вагомості доказів, які можливо отримати в майбутньому при тимчасовому доступі до комп’ютера чи серверу і які оглядаються. Таким чином, при загрузці з CD чи DVD диску, або через підключений USB пристрій . ми рекомендуємо спочатку намагатись вибрати черговість загрузки пристроїв комп’ютера не через настройки BIOS, шляхом вибору меню загрузки пристроїв (інша широко відома назва – «boot menu»), яке визивається при натисканні клавіш «F8», чи «F9», чи «F10», чи «F11», чи «F12» (в залежності від виробника материнських плат) відразу після увімкнення комп’ютера.

Огляд або вилучення з увімкненням комп’ютера та оглядом структури його файлової системи здійснюється декількома способами, але після

закінчення огляду структури файлової системи, системний блок персонального комп’ютера чи сервера необхідно оглянути та провести його вилучення так само, як і у випадку без включення комп’ютера, тобто так само, як і у прикладі наведеному у першому випадку. Як вже зазначалось, огляд чи вилучення з увімкненням комп’ютера та оглядом структури його файлової системи проводиться декількома способами а саме: огляд файлової системи персонального комп’ютеру чи серверу без загрузки операційної системи, що встановлена на комп'ютері, та відключення паролів користувачів операційної системи, що встановлена на комп'ютері і огляд файлової системи персонального комп’ютеру, після чого зокрема слід здійснити:

1) для огляду файлової системи персонального комп’ютера чи серверу доцільно використати загрузочну операційну систему, таку як: «Windows Live CD», чи будьякий «Linux Live CD». В даному випадку необхідно налаштувати загрузку комп’ютера що оглядається так, щоб в першу чергу комп’ютер загружався не зі свого жорсткого диску, а з CD/DVD носія, на якому записана операційна система «Linux Live CD», або «Windows Live CD ». Пріоритет загрузки пристроїв на комп'ютері, файлову систему якого необхідно оглянути, необхідно налаштувати в базовій системі вводу-виводу комп’ютера (на англійській BIOS), а далі вставити диск загрузочною операційною системою в CD чи DVD пристрій, та загрузити операційну систему з нього. При цьому файлова система комп’ютера, що оглядається змінена не буде, а загрузочна операційна система встановиться в оперативно-запам’ятовуючий пристрій, який очиститься від пароля після перезавантаження комп'ютера. Після встановлення в оперативно-запам’ятовуючий пристрій загрузочної операційної системи, працівник правоохоронного органу може отримати змогу оглянути файлову систему персонального комп’ютера чи серверу без обмеження доступу до файлової системи в цілому, чи без обмеження доступу до окремих файлів чи папок. Перед завантаженням загрузочної операційної системи і під час огляду структури файлової системи, необхідно запросити понятих до монітору комп'ютера, що оглядається для того, щоб вони могли побачити й підтвердити перелік дій, що здійснив працівник поліції під час огляду персонального комп’ютера чи сервера. Під час огляду файлів та папок на комп’ютері, що

оглядається доцільним є відеозапис дій працівника поліції на відеокамеру, та здійснити зокрема відеозапис екрану монітору комп'ютера, що оглядається за допомогою спеціального програмного забезпечення, яке може входити в склад програмного забезпечення загрузочного диска. Крім того, усі дії під час огляду комп'ютера необхідно заносити до протоколу огляду, а у разі виявлення файлів, що представляють тактичний, оперативний чи процесуальний інтерес, необхідно заносити до протоколу огляду їх назву, повний шлях до них у файловій системі, розмір у байтах, та бажано створювати для них MD5 суму із спеціальним програмним забезпеченням та подальшим внесенням цієї MD5 суми до протоколу. Треба наголосити, що при створенні MD5 суми для конкретного файлу ця сума у вигляді цифр та знаків буде унікальною для кожного файлу, що відрізняється від іншого файлу хоча б на один байт, а значить ця MD5 сума буде підтверджувати автентичність та незмінність файлу і в подальшому, тобто в ході проведення експертиз, чи під час судового розгляду кримінального провадження по суті в суді. Треба зазначити, що використання загрузочної операційної системи «Windows Live CD» потребує наявності у користувача ліцензії на її використання, але така операційна система має дещо менше можливостей, ніж загрузочна операційна система «Linux Live CD». Крім того, загрузочна операційна система «Linux Live CD» здебільшого є безкоштовною, і може працювати майже з будь-якими файловими системами. Саме тому ми рекомендуємо користуватись загрузочною операційною системою «Linux Live CD ». Як приклад, ви можете завантажити загрузочний диск з операційною системою «Lubuntu» з російськомовного Інтернет ресурсу цієї операційної системи [36], а потім, записавши завантажений образ на диск, користуватись нею для проведення оглядів персонального комп'ютера чи сервера наведеним вище способом;

2) для відключення паролів користувачів операційної системи, встановленої на персональному комп'ютері чи сервері, доцільніше за все використати спосіб наведений вище, але з використанням спеціалізованої загрузочної операційної системи та спеціалізованого програмного забезпечення саме для зміни чи відключення паролів, а вже потім, після перезавантаження комп'ютера, вийняти диск з загрузочною операційною системою, та загрузитись

зі встановленої на персональному комп’ютері чи сервері операційної системи. В даному випадку ми рекомендуємо використовувати загрузочну операційну систему «BartPE» та програмне забезпечення до неї під назвою «Password Renew». Особливістю загрузочної операційної системи «BartPE» є те, що її може створити (зібрати) на основі звичайної операційної системи «Windows» будьякий користувач, але у випадку володіння ліцензійної версії операційної системи «Windows». Враховуючи те, що МВС України активно закупає ліцензійні операційні системи «Windows» – це не викличе суттєвих складнощів у працівників поліції. Під час створення збірки загрузочної операційної системи «BartPE» до її складу необхідно додати програму «Password Renew», за допомогою якої, після встановлення загрузочної операційної системи «BartPE» в оперативнозапам’ятовуючий пристрій персонального комп’ютеру чи серверу, файлову систему якого необхідно оглянути, працівниками поліції буде можливо змінити, чи видалити паролі користувачів з тієї операційної системи, яка вже встановлена на персональний комп'ютер чи сервер, що оглядається. Саму файлову систему комп'ютера, а так само особисті файли користувачів пошкоджено чи змінено не буде.

Але як і в першому випадку, проводити наведені дії комп'ютером, що оглядається необхідно лише в присутності понятих перед монітором комп’ютера, а всі свої дії працівник поліції повинен вносити до відповідного процесуального протоколу згідно положень, зокрема ст.ст. 223, 234, 236, 237, 242, 243, 256 та інших Кримінального процесуального кодексу України, в залежності від обставин вчинення конкретного кримінального правопорушення.

Більшості працівників поліції та тих хто цікавиться проблемами програмного забезпечення при використанні комп’ютерної техніки відома базова система введення і виведення «BIOS» комп’ютера за допомогою якої (на думку багатьох осіб, у тому числі працівників поліції) нібито можна без пошкодження «вскрити» комп’ютерну програму, на яку встановлено пароль для користування нею без володільця. В той же час для питань правозастосовної діяльності, на нашу думку вона у використанні не доцільна, оскільки при її застосуванні все ж таки при огляді комп’ютерної техніки може бути знищена

необхідна для використання у кримінальному провадженні доказова інформація на комп'ютері захищеному паролем.

1.8. Методика основних напрямів виявлення і документування незаконного обігу наркотичних засобів в мережі Інтернет працівниками кіберполіції та інших оперативних підрозділів поліції.

Окрім зазначених у попередніх підпунктах методик виявлення незаконного обігу наркотичних засобів, прекурсорів, їх аналогів, отруйних та сильнодіючих лікарських засобів оперативним працівникам і слідчим слід враховувати й інші можливості використання мережі Інтернет, телекомунікаційних та інших технологій з метою встановлення конкретних осіб, які вчиняють такі види кримінальних правопорушень. На таких можливостях ми зупинимось у цьому підрозділі. Слід зазначити, що останнім часом увага злочинців окрім наркотичних засобів прикута ще й до отруйних і сильнодіючих лікарських засобів за допомогою яких вони готуються та вчиняють кримінальні правопорушення, що замислюють. Вказану тенденцію підтверджує кількість потерпілих від отруєнь, з метою незаконного придбання нерухомості, права на володіння компаніями та комерційними активами, а також при вчиненні зґвалтувань, розбещень, зокрема неповнолітніх, педофілії та ін. все більше використовуються сильнодіючі лікарські препарати.

Так, майже вся аудіо, відео та текстова інформація, яка знаходиться на сторінках сайтів в мережі Інтернет, а так само і розповсюдження наркотичних речовин, отруйних і сильнодіючих лікарських засобів здійснюється його користувачами шляхом формування відповідних пошукових запитів в спеціальних пошукових сервісах. За своєю внутрішньою будовою пошукові сервіси можливо поділити на такі складові частини: відкриту для користувача, та закриту від користувача. В свою чергу, відкриту для користувача частину, умовно можливо поділити на такі зокрема складові частини:

1) одне чи декілька доменних імен Інтернет сайту, через які здійснюється доступ до самого пошукового сервісу;
2) графічна оболонка пошукового сервісу;
3) інструменти для формування пошукових запитів та роботи з ними;

4) блок відображення результатів пошуку інформації за сформованими пошуковими запитами;

В свою чергу закриту від користувача частину можливо, умовно можливо поділити на такі складові частини:

1) пошуковий індекс – перелік доменних імен Інтернет сайтів та конкретної інформації, яка розміщена в мережі Інтернет, що може вивести пошуковий сервіс в блоці відображення результатів пошуку інформації за сформованими пошуковими запитами;
2) пошукові роботи це спеціальні програми, які сканують інформаційний простір мережі Інтернет, та відносять, чи виключають ту чи іншу інформацію до бази даних пошукового сервісу;
3) внутрішні правила, за якими пошукові роботи відносять ту чи іншу інформацію до пошукового індексу пошукової системи;
4) база даних, в якій зберігається аудіо, відео та текстова інформація, яку було включено до пошукового індексу пошукового сервісу.

Майже всі сучасні пошукові сервіси мають потужні пошукові оператори, які дозволяють найбільш точно формулювати запит до пошукового сервісу, враховуючи найменші особливості поведінки її пошукових механізмів. Найбільш популярні критерії пошуку можна задавати з допомогою розширеного пошуку, але володіння пошуковими операторами надає можливість вирішувати складні пошукові задачі.

Нижче будуть розглянуті основні пошукові оператори, які майже не відрізняються у більшості пошукових сервісах. Детальніше про специфіку використання пошукових операторів пошукової системи «Google» працівники поліції можуть знайти на сторінках такого Інтернет – ресурсу, як пошуковий оператор «Google» [Електронний ресурс]. – Режим доступу: http://www.googleguide.com/ advanced_ operators.html або

Оператор	Призначення	Приклад
1	2	3
	пробіл – логічне «AND» або «ТАКОЖ», дає команду для пошукового сервісу на пошук усіх слів, розділених пробілом	хочеш миру готуйся до війни
OR	логічне «ЧИ» дозволяє знайти декілька варіантів слів чи сло восполучень	хочеш миру OR бажаєш миру
|	логічне «ЧИ» дозволяє знайти декілька варіантів слів чи сло восполучень	хочеш миру | бажаєш миру
«»	двійні лапки дозволяють знайти тільки те словосполучення, яке зазначено в них, виключаючи інші варіанти, чи інші слова між зазначеними у словосполученні	«хочеш миру готуйся до війни»
~	символ «~» дає команду для пошукового сервісу на пошук не тільки зазначеного слова, але і його синонімів	~хочеш ~миру ~готуйся ~до ~війни
*****	символ «МНОЖЕННЯ» заміняє одне слово, але можливо вказа ти скільки саме слів може бути між тими, що шукаються	хочеш * * * війни

+	символ «ПЛЮС» дає команду для пошукового сервісу для обов’язкового пошуку слова, перед яким він стоїть	хочеш миру готуйся +до +війни
–	символ «МІНУС» дає команду для пошукового сервісу для обов’язкового виключення з пошуку слова, перед яким він стоїть	хочеш миру війни –хтиш – бачиш

«Всесвітня мережа», або «World Wide Web» (скорочено: WWW; також: всемережжя, ВЕБ або тенета) це найбільше всесвітнє багатомовне сховище інформації в електронному вигляді, тобто десятки мільйонів пов'язаних між собою документів, що розташовані на комп'ютерах розміщених на всій земній кулі. Найбільше, та не єдине. А тому інформація, що представляє тактичний чи оперативний інтерес працівників поліції може бути розміщена також і на FTP серверах і може передаватись за допомогою протоколу передачі даних (англійською мовою – File Transfer Protocol), або FTP.

Протокол передачі файлів (FTP) дає можливість абоненту обмінюватися двійковими і текстовими файлами з будь-ким комп'ютером мережі, що підтримує протокол FTP. Установивши зв'язок з віддаленим комп'ютером, користувач може скопіювати файл з віддаленого комп'ютера на свій, або скопіювати файл з свого комп'ютера на віддалений.

При розгляді FTP як сервісу Інтернет мається на увазі не просто протокол, а саме сервіс доступ до файлів, які знаходяться у файлових архівах. FTP це стандартна програма, яка працює за протоколом TCP, яка завжди поставляється з операційною системою. Її початкове призначення це передача

файлів між різними комп'ютерами, що працюють у мережах TCP/IP, зокрема: на одному з комп'ютерів працює програма сервер, на іншому програма клієнт, що запущена користувачем і з'єднується з сервером та передає або отримує файли через FTPсервіс. Все це розглядається з припущенням, що користувач зареєстрований на сервері та використовує логін і пароль на цьому комп'ютері.

Такі технічні характеристики стали причиною того, що програми FTP стали частиною окремого сервісу Інтернету. Справа в тому, що доволі часто сервер FTP налаштовується таким чином, що з'єднатися з ним можна не тільки під своїм ім'ям, але й під умовним іменем, наприклад, anonymous (анонім). У такому випадку для користувача стає доступною не вся файлова система комп'ютера, а лише деякий набір файлів на сервері, що складають вміст серверу anonymous FTP, тобто публічного файлового архіву. Отже, якщо користувач-злочинець хоче надати у вільне користування файли з інформацією, програмами і таке інше, то йому достатньо організувати на власному комп'ютері, включеному в Інтернет, сервер anonymous FTP. Створення такого серверу це процес доволі простий, програми клієнти FTP вельми розповсюджені, а тому сьогодні публічні файлові архіви організовані в основному як сервери anonymous FTP. Перелік інформації, яка міститься на таких серверах, включає всі аспекти життя: від звичайних текстів до мультимедіа та може використовуватись для виявлення ознак розповсюдження наркотичних речовин.

FTPServer – це серверне програмне забезпечення, яке знаходиться у тієї людини у якої є необхідність скачати відповідну інформацію і за допомогою цього забезпечення здійснюються доступними файли для завантаження по даному протоколу.

Наприклад: Cesar FTP Server, Titan FTP Server, ftpd, ServU Ftp, XLight Ftp Server.

FTPClient – це клієнтська програма за допомогою якої є технічна можливість доступитися до якогось FTPсервера. Наприклад вбудований в операційну систему Windows ftp.exe, Windows Explorer, FTP Voyager, Far manager, Total Commander, Download Master.

Якщо в наявності є спеціальні пошукові сервіси, такі як «Google», призначення яких, здебільшого призначено для пошуку інформації у просторі «Всесвітньої мережі» (або «World Wide Web», чи «WWW»), то є також і спеціальні сервіси пошуку інформації на серверах FTP. У країнах СНД, найбільш зручні та функціональні із них це «FileSearch» та «МАМОНТ» .

Ці пошукові сервіси, призначені для пошуку файлів на FTPсерверах, які доцільно використовувати тоді, коли працівнику відомо, що особою, яка представляє тактичний чи оперативний інтерес, було розміщено інформацію у мережі Інтернет (наприклад, на сторінках Інтернет – сайту, що має електронну адресу виду http://www.sample.ua) певний електронний документ, чи файл). Наприклад, нею може бути файл, створений офісними, чи текстовими програмами – *.doc, *.xls, *.ppt, *.pdf, *.fb2, *.txt та інші. Також, це можуть бути мультимедіа файли : *.avi, *.wmv, *.vob, *.mp4, *.mpeg, *.mkv, *.flv, *.mp3, *.wav, *.wma, *.ogg та інші. Крім цього це можуть бути фотографії, чи графічні зображення – *.bmp, *.png, *.jpg, *.jpeg, *.gif, *.pcx, *.tif, *.tga, *.iff, *.psd та інші.

Наприклад, особою, яка має псевдонім «Stanton», та яка підозрюється у розміщенні в мережі Інтернет повідомлень про збут наркотичних речовин, на сторінках Інтернет – сайту «http://www.sample.ua» було розміщено текстовий файл під назвою «сольлсдпрайс.txt ». В такому випадку слід шукати інформацію про дану особу, використовуючи можливості сервісу та серверів FTP наступним чином:

1) необхідно відкрити спеціальний сервіс пошуку інформації на FTPсерверах. В даному випадку скористаємось таким сервісом, як «МАМОНТ» [26]. Для цього необхідно набрати в адресній строчці WEB – браузера, яким ви користуєтесь, адрес

«http://mmnt.ru», та натиснути клавішу «ENTER»;

2) у поле вводу пошукового запиту сервісу «МАМОНТ» необхідно ввести ім’я файлу, який треба знайти на FTPсервері. В даному випадку – це ім’я файлу «сольлсдпрайс.txt»;

3) трохи нижче поля вводу пошукового запиту сервісу «МАМОНТ», необхідно вибрати режим «Глобальный поиск файлов (ftp://)», натиснувши на відповідну кнопку;
4) після виконання дій, зазначених вище – необхідно натиснути клавішу «ENTER», чи натиснути на кнопку «НАЙТИ», яка розташована правіше від поля вводу пошукового запиту сервісу «МАМОНТ»;
5) після цього, сервіс пошуку інформації на FTPсерверах «МАМОНТ» сформує блок відображення результатів пошуку інформації за сформованими пошуковими запитами,

якщо буде знайдено якусь інформацію, чи проінформує, що у базах даних сервісу «МАМОНТ» нічого не було знайдено;

6) далі, необхідно перевірити FTPсервери, на яких було знайдено файли зі схожою, чи ідентичною назвою. Для цього необхідно скопіювати адрес FTPсервера, який було відображено у блоці результатів пошуку інформації за сформованими пошуковими запитами сервісу «МАМОНТ». Наприклад – це такий адрес: «ftp://83.166.96.170/ALL/Книги/mybooks/як сольлсдпрайс.txt»;
7) для роботи з файлами, які знаходяться на FTPсерверах ми рекомендуємо користуватись файловими менеджерами, таким як «Total Commander» чи «FAR», або такою програмою для операційної системи Windows, як «Download Master».

Після запуску програми «Download Master», необхідно натиснути клавішу «F7», чи перейти в пункт меню «Инструменты», та вибрати поле «FTP Explorer»;

8) у програмі «FTP Explorer», яка відкрилась, у адресну строку необхідно ввести адрес FTPсервера, який ми отримали через сервіс пошуку інформації на FTPсерверах «МАМОНТ»,та який було скопійовано – «ftp://83.166.96.170/ALL/Книги/mybooks/ сольлсдпрайс.txt». Після цього необхідно натиснути клавішу «ENTER»;
9) після цього у програмі «FTP Explorer» повинна відобразитись будова директорій (папок) та файлової системи на FTPсервері, адрес якого було введено. Крім того буде відображено саме ту директорію (папку), де

знаходиться файл, який необхідно було знайти. Тому доцільно вивчити склад даної директорії (папки), та при сприятливих умовах (якщо доступ до фалів FTPсерверу не захищений паролем), завантажити усі файли, які знаходяться в ній;

10) проаналізувати інформацію, яка знаходиться у завантажений файлах, на предмет знаходження в ній даних про особу, яка становить тактичний чи оперативний інтерес. При необхідності – завантажити файли з інших директорій (папок), які також знаходяться на даному FTPсервері; проаналізувати та перевірити і інші FTPсервери, адреси яких було відображено у блоці результатів пошуку інформації за сформованими пошуковими запитами сервісу «МАМОНТ».

Як вже зазначалось вище, велику групу злочинів складають розповсюдження наркотичних речовин, вчинені з використанням сучасних інформаційних технологій та мережі Інтернет. Такі злочини, вчиняються з використанням мережі Інтернет в якості засобу спілкування і реалізації наркотиків покупцеві, що відрізняє від розповсюдженні при фізичному контакті без використання мережі Інтернет. Види розповсюджень вчиняються із використанням закритих і відкритих Інтернет – аукціонів, в яких непомітно для покупця самі продавці роблять ставки, штучно створюючи уяву про участь багатьох покупців у аукціоні, з метою підняти ціну виставленого на аукціон товару. В інших видах збут, продавець виставляє на огляд в мережі Інтернет лише фотографії товару, а після отримання грошей пересилку товару покупцеві здійснює за допомогою «кладу» чи з вигаданого ім’я .

Типовими є ситуації, коли при розповсюдженні наркотиків створюють на сторінках Інтернет – аукціонів та форумів декількох користувачів, які мають різні особисті данні та імена профілів. Також можуть створюватись декілька різних профілів у різних сервісах по збуту. За допомогою цих профілів, створюються сторінки по продажу товарів, але оскільки дуже часто реального товару на руках у злочинців немає, вони використовують однакові графічні зображення, чи цифрові фотографії товару для створення оголошення. Крім того, як правило, використовують відносно одні й ті самі міні зображення для

своїх профілів – так звані «аватарки» що можна використовувати як ідентифікатор особи.

Працівникам поліції вкрай необхідно мати у розпорядженні якомога більше інформації про ту, чи іншу особу, яка представляє оперативний інтерес. А тому пошук в мережі Інтернет усіх створених оголошень та профілів конкретної особи може принести працівникам поліції багато значимої інформації. Наприклад: адреси електронної пошти, якою користується особа, номери телефонів, імена профілів в соціальних мережах, контакти особи. Це можливо тому, що при створенні нових профілів на тих чи інших Інтернет сайтах особа, яка їх створює, залишає свої особисті та контактні данні.

Для реалізації принципу «більша кількість даних створює більшу кількість даних, знайдених з її допомогою», шляхом пошуку ідентичних зображень в мережі Інтернет, необхідно скористатися послугами, що представляють Інтернет сервіси трьох типів: звичайні пошукові сервіси, вбудовані доповнення у звичайні пошукові сервіси, та спеціальні сервіси по пошуку графічних зображень.

Використання пошукових сервісів для пошуку копій графічних зображень :

1) для пошуку копій графічних зображень через звичайний пошуковий сервіс, спочатку необхідно дізнатися ім’я зображення, копії якого необхідно знайти;

2) Для цього по зображенню необхідно натиснути правою клавішою маніпулятору «миша», та у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), чи «показати зображення» (show image). Після цього, ім’я зображення буде передано до адресної строки WEB браузера, в якому ви відкрили дане зображення;

3) отримане ім’я необхідно ввести в поле пошукового запиту того пошукового сервісу, який необхідно використати;

4) далі необхідно проаналізувати результати пошукового запиту у вигляді текстових посилань на Інтернет сайті, на сторінках яких розміщено схоже графічне зображення, та якщо ця функція є у пошуковому сервісі –

переглянути результати пошукових запитів лише у вигляді зображень. Наприклад: «Google Images».

5) якщо необхідно знайти зображення з назвою «get_slimauto_service.jpg» – саме цю назву зображення і необхідно вводити у поле пошукового запиту пошукового сервісу.

Використання спеціальних сервісів для пошуку копій графічних зображень:

1) для пошуку копій графічних зображень через сервіс по пошуку графічних зображень, доцільно скористатись одним із двох сервісів: «TinEye Reverse Image Search» [30], чи «GazoPa similar image search»;

2) для цього необхідно натиснути правою клавішею маніпулятору «миша» по зображенню, копію якого необхідно знайти;

3) у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), а потім ще раз натиснути правою клавішею маніпулятору «миша» по зображенню, яке відкрилося, та вибрати поле меню «зберегти зображення» (save image);

4) далі необхідно перейти на сторінки Інтернет сайту того сервісу по пошуку графічних зображень, з допомогою якого буде здійснено пошук. Наприклад – це сервіс «TinEye Reverse Image Search»;

5) біля поля даного сервісу «Upload your image» розташована кнопка «View» («Пошук», чи «Обзор»), після натискання на яку буде запропоновано вибрати на комп'ютері користувача те зображення, копії якого необхідно знайти;

6) далі, сервісом по пошуку графічних зображень буде виконаний пошук копій вибраного користувачем зображення по своїм базам даних, після чого буде сформовано сторінку відображення результатів пошуку;

7) крім того, в наведеному сервісі «TinEye Reverse Image Search» [30], можливо не загружати зображення з комп'ютера користувача, а ввести лише його адресу в мережі Інтернет, заповнивши поле «Enter image adress», після чого також буде виконаний пошук копій вибраного користувачем зображення по базам даних сервісу.

Використання вбудованих доповнень у звичайні пошукові сервіси для пошуку копій графічних зображень:

1) для пошуку копій графічних зображень через вбудовані доповнення у звичайні пошукові сервіси, доцільно скористатись сервісом, яким надає компанія «Google Inc.» «Google Images»;

2) для цього необхідно натиснути правою клавішею маніпулятору «миша» по зображенню, копію якого необхідно знайти;

3) у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), а потім ще раз натиснути правою клавішею маніпулятору «миша» по зображенню, яке відкрилося, та вибрати поле меню «зберегти зображення» (save image);

4) далі необхідно перейти на сторінки сервісу «Google Images» – з його допомогою буде здійснено пошук копій графічних зображень;

5) праворуч від поля введення пошукового запиту даного сервісу, розміщено маленьке графічне зображення фотоапарату, після натискання на яке буде запропоновано вибрати на комп'ютері користувача те зображення, копії якого необхідно знайти;

6) далі, сервісом «Google Images» буде виконаний пошук копій вибраного користувачем зображення по своїм базам даних, після чого буде сформовано сторінку відображення результатів пошуку, та буде сформовано сторінку відображення результатів пошуку;

7) крім того, в наведеному сервісі «Google Images», можливо не загружати зображення з комп'ютера користувача, а ввести лише його адресу в мережі Інтернет, чи його назву, якщо вона відома, заповнивши поле пошукового запиту, після чого також буде виконаний пошук копій вибраного користувачем зображення по базам даних сервісу, та буде сформовано сторінку відображення результатів пошуку.

Як вже зазначалось вище, певна кількість даних створює ще більшу кількість даних, знайдених за її допомогою. Тобто якщо про особу невідомо нічого, то без цього пошук є неможливим.

У випадках коли про особу відома будь-яка інформація, наприклад, прізвище, ім'я та по батькові, чи адреса електронної пошти, чи ім'я в сервісі

Skype, чи нік Телеграм, чи дата народження, чи навчальний заклад та рік, в якому дана особа закінчила навчання, або є інша інформація – це може надати можливість працівникам органів поліції знайти ще більшу інформацію про дану особу, навіть використовуючи лише можливості соціальних мереж. Для цього необхідно ввести вказані данні про особу в пошукову систему, наприклад «Google». Переглядаючи отримані попередні пошукові результати, необхідно перевіряти й інші, і перш за все необхідно перейти на сторінки профілів даної особи в соціальних мережах, якщо такі є. Для цього доцільно буде послідовно ввести в пошукову систему прізвище, ім'я та по батькові особи, та назву соціальної мережі, наприклад: «Іваненко Іван Іванович facebook», після перевірки результатів – «Іваненко Іван Іванович instagram», і так само далі працювати з іншими соціальними мережами. Якщо є відомості про особисті дані особи лише частково, в подальшому доцільно буде застосувати ще й інші три способи пошуку: через пошуковий сервіс, через фільтри соціальної мережі, та комбінований. Зупинимось на кожному із них.

Пошук інформації про особу в соціальній мережі, з використанням пошукового сервісу:

1) необхідно ввести в пошукову систему спочатку всю відому і наявну інформацію про особу та назву соціальної мережі. Наприклад: «Гадюченко Григор Григорович 11.11.1981 +380661235456 Харків Gadyuka@i.ua Facebook»;

2) якщо це не принесло бажаних результатів, то в подальшому доцільно буде ввести по черзі частку інформації про особу, та назву соціальної мережі. Це пов'язано з тим, що особа, яка цікавить правоохоронців, може створювати в соціальних мережах профілі з іншими прізвищами та частково, або повністю зміненими особистими даними;

3) наприклад працівникам органів поліції відомі дата народження та номер телефону особи, про яку необхідно отримати певну інформацію, отже для цього доцільно використати відомі дані, для чого необхідно ввести в пошуковій системі: «11.11.1981 +380661235456 facebook», потім «11.11.1981 facebook», потім «+380661235456 facebook», потім «11.11.1981 +380661235456 instagram» та ін.;

4) проаналізувати отримані результати.

Пошук інформації про особу в соціальній мережі, з використанням пошукових фільтрів самої соціальної мережі:

1) пошук може вестись всередині самих соціальних мереж, для чого необхідно зареєструватись в соціальній мережі, та створити власний профіль;

2) цей метод пошуку дуже доцільний завдяки тому, що у кожній соціальній мережі є функціональна система пошуку з багатьма фільтрами. Фільтри в соціальних мережах – це пошук інформації по відповідній умові, наприклад: по віку, по місцю народження, по вподобанням, по назві навчального закладу, тощо. В системах пошуку всередині соціальних мереж можна шукати особу тільки по прізвищу, чи по віку, чи по даті народження, чи по місту народження, чи по ставленню, наприклад до вживання спиртних напоїв. Список фільтрів пошуку, які можна використати при пошуку певної особи є дуже великий та різноманітний.

За результатами пошуку також можливо виявити сліди IP адреси користувача.

IPадреса (Internet Protocol address) — це унікальний числовий номер, або ідентифікатор мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP. Прикладом такої мережі є Інтернет.

Будь-яка IP-адреса складається з чотирьох 8бітних чисел, які називають октетами (вад латинського «ОКТ» вісім). Найпростішим прикладом IP-адреси може бути адреса 192.168.0.31. Будь-кому доменному імені WEB сайту, чи конкретному користувачу мережі Інтернет відповідає певний IP-адрес. Процес перетворення доменного імені у IP-адресу виконується DNS сервером.

IP-адреса складається з двох частин: номера мережі і номера вузла. У разі ізольованої мережі її адреса може бути обрана адміністратором зі спеціально зарезервованих для таких мереж блоків адрес (14.14.0.0 / 6, 192.192.0.0 / 16 або 192.111.1.1 / 12). Але у разі, коли мережа повинна працювати як складова частина Інтернету, то адреса мережі видається провайдером або регіональним Інтернет реєстратором (Regional Internet Registry, RIR). Згідно з даними на сайті IANA існує п'ять RIR: ARIN, обслуговуючий Північну Америку; APNIC, обслуговуючий країни ПівденноСхідної Азії; AfriNIC, обслуговуючий країни Африки; LACNIC, обслуговуючий країни Південної Америки і басейну

Карибського моря; та RIPE NCC, обслуговуючий Європу, Центральну Азію, Близький Схід. Ті регіональні реєстратори, які отримують номери автономних систем і великі блоки адрес у IANA, а потім видають номери автономних систем та блоки адрес меншого розміру локальним Інтернет реєстраторам (Local Internet Registries, LIR), зазвичай є великими провайдерами.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP адресу. Кінцевий вузол також може входити в кілька IP мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. Саме тому, завдяки наявності IP адреси особи, яка представляє оперативний інтерес, можливо встановити місцезнаходження точки її доступу до Інтернету (країну, місто), та назву провайдера, який надає особі можливість такого доступу до Інтернету.

Головним завданням, в даному випадку, виступає спосіб отримання IP адреси особи, яка представляє оперативний інтерес для працівників поліції. Основними способами є такі, як: запити до адміністрації звичайних (комерційних чи некомерційних) Інтернет сайтів та використання легендованих Інтернет сайтів.

Запити до адміністрації звичайних (комерційних чи некомерційних) Інтернетсайтів – є доцільними у тому випадку, коли працівнику поліції відомо, що саме на цьому Інтернетсайті зареєстрована та веде переписку (чи іншу діяльність, пов’язану використанням можливостей конкретного Інтернетсайту) особа, яка представляє тактичний чи оперативний інтерес. Запит є доцільним тому, що майже у всіх сучасних «двигунах» Інтернетсайтів та Інтернетфорумів є функція фіксації IPадреси кожного конкретного користувача, який зареєстрований на даному Інтернетресурсі, чи користувача, який заходив до Інтернетресурсу анонімно. У запиті необхідно указати підстави та причини звернення до адміністрації, та ім’я (вигадане чи справжнє) тієї особи, щодо якої необхідно узнати IPадресу. Також доцільним є вказати в запиті настання відповідальності за розголошення відомостей, що містяться у запиті.

Використання легендованих Інтернетсайтів – є доцільними у тому випадку, коли працівнику органів поліції не вдалося у інший спосіб отримати

IPадресу особи, яка представляє оперативний інтерес, чи використання іншого способу отримання IP адреси ризикованим (наприклад – витік інформації). У даному випадку головними завданнями є: використання достатньо легендованого сайту, який би не виглядав «порожнім», чи не був щойно створеним, та обережність при спрямуванні особи, яка представляє тактичний чи оперативний інтерес на даний Інтернетресурс. Обережність повинна виявлятись в тому, що необхідно пам'ятати про те, що настирливість у намаганнях спрямувати особу до легендованого сайту може її просто відлякати від нього, та навіть заставити її «залягти на дно». Тактично правильним рішенням буде визначити вподобання особи, визначити коло Інтернетресурсів, якими особа користується, дізнатися адреси електронної пошти особи, а потім, нібито не для неї, залишати послання на легендований Інтернетсайт. Це можуть бути графічні зображення малого розміру, що зумовлює бажання натиснути на них для того, щоб вони збільшились у розмірі, але замість цього – це буде масковане посилання на легендований Інтернетсайт. Так само посилання можливо замаскувати під графічне зображення відео кліпу, чи аудіо запису, тощо. Звісно, на самому легендованому сайті повинна бути присутня функція фіксації IPадрес користувачів, які до нього зайшли.

Розглянемо приклад, в якому працівнику поліції відомо, що IPадреса особи, яка розповсюджує відеофільми порнографічного характеру, має наступний ідентифікатор: 178.151.128.221 :

1. для отримання похідних даних від IPадреси, зручно скористатись сервісом «WHOIS», наприклад таким, який надає Інтернетресурс «2IP.UA»;
2. для цього необхідно перейти на сторінку Інтернетресурсу за адресою «http://2ip.ua/whois», та у поле «IP адрес или домен» ввести ідентифікатор IPадреси, яка представляє оперативний інтерес, після чого необхідно нажати клавішу «ENTER». У даному випадку – це IPадрес: 178.151.128.221;
3. після цього буде сформовано сторінку, на якій буде відображено наступну інформацію:

ПАРАМЕТР	ЗНАЧЕННЯ	ПОЯСНЕННЯ
IP	178.151.128.221	IPадреса, стосовно якої був виконаний запит
ХОСТ	224.128.151.178.triol an.net	IPадреса серверу, через який користувач IPадреси 178.151.128.221 здійснює доступ до Інтернету
МІСТО	Харьков	Місто, де знаходиться користувач IPадреси 178.151.128.221
КРАЇНА	Ukraine	Країна, де знаходиться користувач IPадреси 178.151.128.221
IPдіапазон	178.151.128.0 178.151.128.255	Діапазон IPадрес, до якого належить IPадреса 178.151.128.221
НАЗВА ПРОВАЙДЕРА	Kharkov , Odesskaya	Інтернетпровайдер, через який користувач IPадреси 178.151.128.221 здійснює доступ до мережі Інтернет

4. далі, використовуючи отримані дані, а головне – країну, місто та назву Інтернетпровайдеру, через якого користувач IPадреси 178.151.128.221 здійснює доступ до мережі Інтернет, від імені правоохоронного органу формується запит до Інтернетпровайдеру, в якому ставиться питання про те, до якої конкретної фізичної адреси

прив’язана IPадреса користувача. В даному випадку – до якої фізичної адреси відноситься IPадреса 178.151.128.221;

5) після отримання відповіді на запит, працівники органу внутрішніх справ приймають рішення про подальші дії: необхідність проведення негласних слідчих (розшукових) дій, обшуку чи інших слідчих дій;
6) аналіз отриманих результатів.

Отриману та виявлену в ході проведення пошуків та виділення результатів мережі Інтернет можливо фіксувати за допомогою програмних засобів ПК Знімком екрану та складанням протоколу «огляду мережі Інтернет» в процесуальному порядку передбаченому КПК України.

2. Встановлення коштів, здобутих від незаконного обігу наркотиків, психотропних речовин, їх аналогів, прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів

Наркоманія і наркобізнес утворюють одну з основних транснаціональних проблем сучасного суспільства. Нелегальний обіг наркотичних засобів, психотропних речовин та прекурсорів в Україні і в світі набуває дедалі значніших масштабів. Кошти отримані в сфері наркобізнесу складають величезні суми, які злочинці намагаються легалізувати, що негативно впливає на економічний стан держави. Злочини вказаної категорії є високолатентними, тому кількість зареєстрованих кримінальних проваджень досить низька. Така ситуація складається зокрема через те, що ці злочини вчиняються організованими злочинними групами, які намагаються здійснювати ефективний супротив правоохоронним органам, їх діяльності направленій на виявлення, розкриття та розслідування злочинів, зокрема таких видів. Тому під час досудового розслідування від працівників правоохоронних органів вимагається не лише наявність професійної майстерності кожного, але й організації належного рівня взаємодії слідчих, детективів (в порядку експерименту) та оперативних працівників. Дані методичні рекомендації напрацьовані з метою надання також допомоги слідчим, детективам та працівникам оперативних підрозділів органів поліції у виявленні, розкритті та розслідуванні злочинів, пов’язаних з використанням коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів відповідальність за які передбачена ст. 306 КК України.

2.1.Кримінально-правова характеристика використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів відповідальність за яке передбачена ст. 306 КК України

2.1.1. Кримінально-правова характеристика порушень правил обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів

Згідно з чинним законодавством, розміщення коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів у банках, на підприємствах, в установах, організаціях та їх підрозділах або використання таких коштів для придбання об'єктів, майна, що підлягають приватизації, чи обладнання для виробничих чи інших потреб, або використання таких доходів (коштів і майна) з метою продовження незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів; а також ці ж дії вчинені повторно або за попередньою змовою групою осіб, або у великих розмірах (під великим розміром слід розуміти кошти, сума яких становить двісті та більше неоподаткованих мінімумів доходів громадян), – кваліфікують за ст. 306 Кримінального кодексу України, як *використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів*.

Поряд з цим закон про кримінальну відповідальність містить ст. 209 КК, яка передбачає відповідальність за легалізацію (відмивання) доходів, одержаних злочинним шляхом.

Відмінність злочину, передбаченого ст. 306 КК від ст. 209 КК полягає у джерелах надходження доходів, предметі злочину та деяких ознаках об’єктивної сторони. Але, у ряді випадків легалізація коштів чи майна потребує кваліфікації за сукупністю злочинів, передбачених ст.ст. 209 і 306 КК України.

У контексті ст. 306 КК України особа одержує гроші, що відмиваються, в результаті вчинення злочинів, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів тобто злочинів, передбачених Розділом XIII Кримінального кодексу України. Якщо «брудні» гроші отримані від іншої злочинної діяльності, відповідальність настає за ст. 209 КК України.

Відмивання грошей – це злочинна діяльність, нерідко у міжнародному масштабі, що характеризується умисним приховуванням справжнього джерела отримання коштів чи майна шляхом незаконного їх використання з метою легалізації злочинних доходів.

Основний безпосередній *об'єкт злочину*, передбаченого ст. 306 КК України – це порядок здійснення господарської чи підприємницької діяльності, який встановлений для протидії наркобізнесу та залученню в економіку «брудних» коштів, а також виконання Україною взятих на себе міжнародно-правових зобов'язань.

Предметом злочину є: 1) кошти, здобуті від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що використовуються з метою їх відмивання; 2) майно і кошти, здобуті від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що використовуються з метою продовження цієї злочинної діяльності.

Об'єктивна сторона злочину передбачає здійснення кількох альтернативних дій.

1. Розміщення коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів у банках, на підприємствах, в установах, організаціях та їх підрозділах. При цьому розміщення коштів означає внесення їх на рахунок банку, переведення коштів з одного рахунка на інший, внесення їх у фонди підприємств, установ,

організацій чи у фонди їх філій та інші дії, пов’язані з використанням коштів, отриманих внаслідок наркобізнесу.

2. Використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, для придбання об’єктів, майна, що підлягають приватизації, або обладнання для виробничих чи інших потреб. Таке використання коштів може мати місце, у процесі викупу, тендера або на аукціоні особисто або через посередника. Придбанням обладнання для виробничих або інших потреб є купівля апаратури, механізмів, приладів та ін.

3. Використання таких доходів (коштів і майна) з метою продовження незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів означає фінансування злочинної діяльності у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів. Таке фінансування діяльність може бути пов’язано з внесенням або зняттям депозиту або вкладу, переказом грошей з рахунка на рахунок, обміном валюти і інше, якщо ці дії здійснюються для продовження заняття незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

Однак використання доходів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів з метою продовження такого обігу не є відмиванням «брудних» грошей. Легалізація доходів не може вчинятися у сфері незаконної діяльності, в тому числі, і у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

Суб’єкт злочину загальний, тобто, за його вчинення може відповідати фізична осудна особа, яка вчинила злочин у віці 16 років.

Суб'єктивна сторона характеризується прямим умислом. Тобто, винний має усвідомлювати незаконне походження коштів, здобутих внаслідок незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів. Обов'язковою ознакою суб'єктивної сторони є *мета* злочину: продовження незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

У випадках, коли «брудні» кошти розміщують в різних банках, підприємствах, або на них приватизовано два чи більше об'єкта, або ж профінансовано дві чи більше особи, залучені до незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів, навіть у випадку коли ці кошти отримані від однієї операції з наркотиками та ін., – злочин кваліфікують за ч. 2 ст. 306 КК за ознакою *повторність*. Головним визначенням повторності є неодноразовість операцій з коштами, здобутими від незаконного наркообігу та (або) обігу отруйних і сильнодіючих речовин.

Передбачені ч. 1 ст. 306 КК дії визначаються вчиненими у *великому розмірі*, якщо їх сума становить двісті та більше неоподаткованих мінімумів доходів громадян, не тільки коли ці кошти є предметом одного епізоду злочину, а й у випадках неодноразового використання коштів, коли їхня вартість у сукупності становить зазначену суму.

3. Особливості організації виявлення, розкриття та розслідування злочинів, передбачених ст. 306 КК України

3.1. Особливості початкового етапу розслідування кримінальних проваджень щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів

Початковий етап досудового розслідування кримінальних проваджень, розпочатих за ознаками використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів, має деякі особливості. Найчастіше кримінальні провадження даної категорії порушуються за результатами проведення негласних слідчих (розшукових) дій або оперативно-розшукових заходів.

Початок досудового розслідування за ст. 306 КК України зазвичай передує розслідування злочину, передбаченого Розділом XIII Кримінального кодексу України: «Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення», а саме ст.ст. 305, 307, 308, 310 – 313, 317 – 320, 322 КК України.

Орієнтуюча інформація про використання «брудних» коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів може бути одержана органами поліції і правоохоронними органами із різних джерел: 1) з відомостей, одержаних в ході здійснення негласних слідчих (розшукових) дій і оперативно-розшукових заходів відповідними оперативними підрозділами поліції та інших правоохоронних органів; 2) з повідомлень службових осіб, працівників установ, які є суб'єктами фінансового контролю (Держфінмоніторингу, банків, інших

установ); 3) з заяв, повідомлень громадян чи засобів масової інформації; 4) з матеріалів кримінального провадження про первинний (основний) злочин.

Однак, слід мати на увазі, що для початку досудового розслідування за ст. 306 КК, необхідно встановити, що «брудні» кошти здобуті саме від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів. Саме тому на практиці, інформація щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів отримується слідчим вже при розслідуванні кримінальних справ, порушених за статтями 305, 307, 308, 310 – 313, 317 – 320, 322 Кримінального кодексу України. Це обумовлено складом злочину, передбаченому ст. 306 КК України. Тому на стадії порушення кримінальної справи обов'язковому встановленню підлягають наступні *обставини*:

1) що обвинувачена (підозрювана) особа саме в результаті вчинення злочину у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів отримувала конкретні встановлені на досудовому слідстві кошти;

2) що обвинувачена (підозрювана) особа усвідомлювала незаконне походження цих грошей чи майна; що обвинувачена (підозрювана) особа ставила за мету використання «брудних» коштів для продовження незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів;

3) що обвинувачена (підозрювана) особа вчинила конкретні дії щодо використання «брудних» коштів і в чому саме ці дії полягали: а) в розміщенні грошей шляхом внесення їх на встановлений в ході досудового розслідування рахунок банку; б) в проведенні встановленої досудовим розслідуванням операції по переведенню грошей з одного банківського рахунку на інший; в) у

встановленому слідством факті внесення конкретних коштів у фонди підприємств, установ, організацій та ін.

Необхідно враховувати, що можливість отримання коштів від незаконного обігу наркотиків завжди мають особи, які вчиняють злочини цієї категорії саме *з метою збуту* наркотичних засобів, психотропних речовин чи прекурсорів (адже гроші отримуються в результаті збуту наркотичних засобів, психотропних речовин чи прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів).

Слід розглянути *типові слідчі ситуації*, що виникають на початку досудового розслідування щодо використання коштів, отриманих від незаконного обігу наркотичних засобів, психотропних речовин їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів. Доцільно виділити такі слідчі ситуації:

1) інформація про використання злочинних коштів надходить до слідчого за результатами проведення негласних слідчих (розшукових) дій або від оперативних працівників, які провели перевірочні дії і підготували первинний матеріал;

2) інформація про використання злочинних коштів одержана слідчим при розслідуванні кримінального провадження про основний злочин.

Перша слідча ситуація виникає, коли при проведенні оперативно-розшукових заходів, а саме при знятті інформації з каналів зв'язку, включаючи обмін електронними повідомленнями, отримується непроцесуальна (орієнтуюча) інформація, щодо використання коштів отриманих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

Для того, щоб відомості, отримані при проведенні такої *тактичної операції* можна було використовувати в якості доказів по кримінальному провадженню, їх легалізують шляхом процесуального оформлення у встановленому законом порядку. Легалізовані оперативно-технічні матеріали

(зазвичай аудіозаписи) надходять до слідчого. Слідчий визнає їх речовими доказами і додає до матеріалів кримінального провадження. Підкреслимо, що відомості, щодо використання злочинцями «брудних» грошей отримуються, коли оперативні працівники, детективи і слідчий вже знають про вчинення основного (первинного) злочину, пов'язаного із незаконним обігом наркотичних засобів.

Проведенню тактичної операції, повинно передувати колективне моделювання реально можливих ситуацій її реалізації слідчими, детективами і оперативними працівниками. З урахуванням тієї або іншої ситуації здійснюються розрахунки сил і засобів, необхідних для успішного проведення операції, основною метою якої є *отримання доказів* у кримінальному провадженні. Тобто, у цій слідчий ситуації головним напрямом діяльності слідчого, детектива і оперативного співробітника є не тільки збір, а й грамотне процесуальне закріплення доказів використання коштів отриманих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів. Крім того, важливим аспектом є вибір тактики, способу і часу проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій і оперативно-розшукових заходів.

У *другій слідчій ситуації* інформація щодо вчинення злочину, передбаченого ст. 306 КК отримується безпосередньо слідчим процесуальним шляхом при проведенні слідчих (розшукових) дій, або негласних слідчих (розшукових) дій по основному кримінальному провадженню. У цій ситуації дуже важливим є використання попереднього досвіду щодо оперативного супроводження кримінального провадження оперативними працівниками в суді. (Така можливість є за рахунок впровадження посад детективів).

В обох слідчих ситуаціях на етапі початку кримінального провадження необхідно отримати наступну інформацію:

1) документальне підтвердження факту вчинення будь-яких дій або угод з метою використання доходів, отриманих від незаконного обігу наркотиків;

2) підтвердження факту одержання коштів (грошей чи майна), з яким вчинено відповідні дії, саме внаслідок вчинення злочину у сфері наркобізнесу.

Для цього, з метою документального підтвердження обставин, щодо використання коштів, отриманих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів, необхідно провести такі заходи:

– з дозволу (ухвали) слідчого судді, в порядку, встановленому ч. 5 ст. 97 КПК України здійснити оперативно-технічні заходи для отримання фактичних даних про обставини, які можуть бути використані як докази у кримінальному провадженні, у тому числі й шляхом зняття інформації з каналів зв'язку, включаючи обмін електронними повідомленнями;

– направити відповідні ухвали слідчого судді щодо запитів до відділень операторів (провайдерів) телекомунікації (Інтернет та мобільного зв’язку, ВАТ «Укртелеком»), тощо, з метою перевірки та підтвердження відносин між підозрюваними та іншими особами, причетними до вчинення злочину;

– витребувати з банківських установ, в яких відкрито рахунки осіб, які перевіряються, дані про рух грошових коштів по рахунках за конкретний період;

– вилучити з банківських установ, в яких відкрито рахунки підозрюваних осіб, записи відео спостереження з банкоматів для підтвердження зняття грошей підозрюваною особою з відповідного рахунку у конкретний період;

– отримати пояснення у причетних осіб та вилучити необхідні документи, що підтверджують використання коштів, отриманих від наркобізнесу;

– направити запити до бюро технічної інвентаризації щодо нерухомого майна, яке перебуває у власності осіб, підозрюваних у використанні доходів від наркобізнесу, а також у близьких їм осіб;

– витребувати з фіскальних органів всі відомості, що стосуються діяльності конкретних фізичних осіб та сплати ними необхідних податків;

– отримати показання інших поінформованих осіб щодо обставин вчинення використання коштів, отриманих від наркобізнесу;

– звернутися із запитом до Державної фіскальної служби України з метою перевірки інформації, або отримання додаткової інформації з Банку даних про сумнівні фінансові операції;

– направити запити до сервісних центрів МВС України і Національної поліції України щодо попередньої судимості особи, до оперативних та інших обліків, а також витребувати інші документи і матеріали, що характеризують особу, зокрема, перевірити можливість її причетності до діяльності відомих злочинних груп або організацій та ін.

Для того, щоб отримані відомості можна було використовувати в якості доказів у кримінальному провадженні, їх оформлюють згідно з чинним кримінальним процесуальним законодавством. Оперативно-технічні матеріали (аудіо- чи відеозаписи) надсилаються до слідчого. Слідчий визнає їх речовими доказами і долучає до матеріалів кримінального провадження.

3.2. Обставини, що підлягають встановленню і наступний етап розслідування кримінальних проваджень щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів

Початок досудового розслідування за ознаками ст. 306 КК України зазвичай передує розслідування (або встановлення факту вчинення) основного злочину, тобто злочину, передбаченого Розділом XIII Кримінального кодексу України: «Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення», статтями 305, 307, 308, 310 – 313, 317 – 320, 322.

Коли по основному злочину кримінальне провадження вже розслідується, то на етапі початку досудового розслідування за статтею 306 КК України:

а) особи, щодо яких проводиться досудове розслідування нове кримінальне провадження вже має процесуальний статус підозрюваного;

б) в матеріалах основного кримінального провадження є докази вчинення підозрюваним злочину у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів;

в) наявні фактичні данні, що підтверджують використання підозрюваним чи іншими причетними особами коштів здобутих від незаконного наркообігу.

Мають місце випадки, коли кримінальне провадження по основному злочину починається паралельно із кримінальним провадженням за ст. 306 КК України. Незалежно від слідчої ситуації, що склалася на початковому етапі, на наступному етапі досудового розслідування кримінального провадження за ст. 306 КК з'ясуванню підлягають наступні *обставини*:

1) факт отримання відповідних коштів при вчиненні злочину у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів;

2) об'єктивна сторона злочину: тобто, які конкретні дії, передбачені диспозицією ст. 306 КК, були вчинені особою і у чому вони полягали;

3) на що саме використовувались кошти, їх розмір, час одержання і місцезнаходження;

4) конкретні данні щодо джерела походження коштів, а саме:

а) наявність або відсутність кримінального провадження по основному злочину;

б) конкретні обставини злочину, в результаті яких здобуті злочинні кошти;

в) причинно-наслідкові зв'язки між первинним (основним) злочином щодо незаконного обігу наркотиків і використанням «брудних» коштів;

г) канали надходження коштів здобутих від наркобізнесу;

5) обставини, щодо способу використання «брудних» коштів:

а) які конкретно фінансові операції було здійснено, де, коли і ким;

б) чи використовувались банківські рахунки і які саме, чи мало місце перерахування грошових коштів за кордон;

в) розмір, частота, періодичність здійснення фінансових операцій;

г) сліди, що залишилися в документах щодо конкретних дій осіб, які використовували «брудні» кошти;

6) обстановка, час і місце здійснення використання «брудних» коштів:

а) час здійснення кожної фінансової операції;

б) упродовж якого терміну здійснювалися такого роду злочинні дії;

7) час виникнення майнових прав на рухоме і нерухоме майно;

8) характеристика особи злочинця: вік, стать, рівень освіти, фахові, професійні, ділові та моральні якості;

8) коло осіб, які залучалися до вчинення злочину, роль кожного з них, мотив їх поведінки, причетність до вчинення основного (первинного) злочину, джерела і ступінь їх обізнаності про обставини злочинного отримання коштів, час отримання такої інформації (до або після використання злочинних доходів);

10) обставини, що впливають на ступінь та характер відповідальності кожного зі співучасників;

11) причини та умови, що сприяли вчиненню злочину.

3.3. Особливості взаємодії у сфері виявлення, документування і розслідування фактів легалізації доходів, здобутих від незаконного обігу наркотиків

Важлива орієнтуюча, а іноді і доказова інформація, щодо легалізації доходів, здобутих від незаконного обігу наркотиків може бути отримана слідчим, детективом, оперативним працівником й з інших джерел, таких як Національне центральне бюро (НЦБ) Інтерполу в Україні і Державної служби фінансового моніторингу (Держфінмоніторинг).

Співробітництво правоохоронних органів України з правоохоронними структурами іноземних держав у рамках **Міжнародної організації кримінальної поліції – Інтерпол, що передбачається Інструкцією про порядок використання правоохоронними органами України**

інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол», *затвердженої* спільним наказом МВС України, Офісом Генерального прокурора, Національним антикорупційним бюро України, Службою безпеки України, Державним бюро розслідувань, Міністерством фінансів України, Міністерством юстиції України **від 17.08.2020 р. № 613/380/93/228/414/510/2801/5.**

При досудовому розслідуванні злочинів, передбачених ст. 306 КК України, можливості вказаного Департаменту МВС України можна використовувати для отримання інформації з таких питань: окремих суб'єктів господарювання; окремих аспектів діяльності певної фізичної або юридичної особи; перевірки автентичності і факту можливого використання злочинцями підроблених документів; ідентифікації осіб, підозрюваних у легалізації доходів, здобутих від незаконного обігу наркотиків за обліками поліції зарубіжних країн; міжнародного розшуку каналами Інтерполу осіб, котрі підозрюються або обвинувачуються у вчиненні злочинів, пов'язаних з незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів.

Як правило, банківську або комерційну таємницю становлять і відомості про відкриття фізичними особами, в тому числі громадянами України та юридичними особами фінансових рахунків у зарубіжних банках, а також наступні відомості: про рух коштів по таких рахунках, про укладання угод між українськими та закордонними юридичними особами. Такі відомості можуть повідомлятися іноземними правоохоронними органами лише після розгляду верховним органом юстиції (прокуратурою) запитуваної держави в порядку надання правової допомоги в кримінальному провадженні, після офіційного звернення до них Генеральної прокуратури України.

У процесі виявлення, документування і розслідування злочинів, щодо легалізації доходів здобутих від незаконного обігу наркотиків, слідчий,

детектив, оперативний працівник каналами Інтерполу, може отримати наступну інформацію:

– офіційну назву юридичних осіб, зареєстрованих за кордоном, їх юридичну адресу, номер і дату реєстрації;

– прізвища, імена фізичних осіб-керівників (в окремих випадках засновників, акціонерів);

– напрями діяльності, розмір статутного капіталу, поточний фінансовий стан юридичної особи;

– про протиправну діяльність юридичних та фізичних осіб.

Крім того, можливе отримання відомостей про наявність нерухомості та іншої форми власності за кордоном у підозрюваних (обвинувачених) осіб, при умові, якщо відомо конкретне місцезнаходження об'єктів власності (держава, місто, організація).

Запити з питань виявлення, документування і розслідування злочинів щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, що надсилаються до Депатраменту міжнародного поліцейського співробітництва МВС України (колишнє НЦБ Інтерполу) повинні містити такі відомості:

1) конкретні факти, які є підставою для звернення до правоохоронних органів зарубіжних держав: наявність кримінального провадження, її номер, дата реєстрації в ЄРДР, стаття кримінального кодексу за якою (якими) інкримінується злочинна дія; оперативно-розшукова справа, її номер; перевірка оперативної інформації, номер оперативного повідомлення;

2) анкетні данні особи, щодо якої робиться запит, її процесуальний статус;

3) обставини злочину із зазначенням способу його вчинення підозрюваним;

4) повні реквізити зарубіжних фірм та інших об'єктів, які підлягають перевірці, надаються мовою держави, де вони зареєстровані або англійською, французькою чи іспанською;

5) місце або регіон реєстрації суб’єкта підприємницької діяльності;

6) зв'язок зарубіжного суб’єкта з перевіркою, що виконується в Україні;

7) конкретні питання на які передбачається отримати відповідь.

Слід наголосити, що можливості НЦБ Інтерполу в Україні, як правило використовуються правоохоронними органами під час проведення негласних слідчих (розшукових) дій та оперативно-розшукових заходів як до початку проведення кримінального провадження, так і під час досудового розслідування. В більшості випадків матеріали і інформація, які отримуються каналами Інтерполу (через новий Департамент Міжнародного поліцейського співробітництва МВС України), носять орієнтуючий характер і можуть використовуватися слідчим, детективом, оперативним працівником лише в якості непрямих доказів і лише в окремих випадках. Питання проведення окремих слідчих (розшукових) дій, екстрадиції та отримання відомостей про рух коштів на банківських рахунках на території зарубіжних країн вирішуються в порядку надання правової допомоги і належать до компетенції Генеральної прокуратури України. Слідчий, детектив або оперативні працівники звертаються через відповідних прокурорів, які здійснюють нагляд, до Офісу Генерального прокуратура з клопотанням про підготовку звернення до центрального органу юстиції (прокуратури) зарубіжної держави із запитом про надання правової допомоги.

Розглянемо можливості використання інформації отриманої слідчим від Державної служби фінансового моніторингу.

Держфінмоніторинг створено, як підрозділ фінансової розвідки, призначений для протидії відмиванню коштів та фінансуванню тероризму. Він є сполучною ланкою в загальнодержавній системі протидії злочинам, передбаченим ст.ст. 209, 209-1, 306 КК України. Підкреслимо, що основним завданням підрозділів фінансової розвідки є не виявлення злочинців, а попередження легалізації злочинних доходів, шляхом розроблення ефективних заходів, переважно фінансового характеру та контролю за їх виконанням.

Водночас підрозділ фінансової розвідки є ефективним постачальником інформації про кошти, які могли бути отримані в результаті злочинної діяльності, і таким чином сприяє розслідуванню предикатних злочинів щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів.

Порядок надання Держфінмоніторингом правоохоронним органам інформації про сумнівні операції регулюються наступним нормативними актами:

1) постанова Кабінету Міністрів України від 29 липня 2015 року № 537 «Про затвердження Положення про Державну службу фінансового моніторингу України;

2) наказ Міністерства фінансів України (Мінфін), Міністерства внутрішніх справ (МВС), Служби безпеки України від 11.03.2019 № 103/162/384 «Про затвердження Порядку надання та розгляду узагальнених матеріалів».

При розслідуванні кримінального провадження за ст. 306 КК України, щодо використання коштів здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, слідчий, детектив, працівник оперативного підрозділу повинні знати, що відповідно до Положення про Державну службу фінансового моніторингу України основними завданнями Держфінмоніторинга є:

– участь в реалізації державної політики у сфері запобігання та протидії легалізації доходів, одержаних злочинним шляхом;

– створення та забезпечення функціонування єдиної державної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом;

– забезпечення в установленому порядку представництва України в міжнародних організаціях з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Тобто, при розслідуванні злочинів, передбачених ст. 306 Кримінального кодексу України слідчий має можливість отримати необхідну інформацію при взаємодії з Держфінмоніторингом і НЦБ Інтерполу, важливість якої важко переоцінити.

3.3. Особливості проведення обшуку при розслідуванні злочинів передбачених ст. 306 КК України

Обшуки після винесення ухвали слідчим суддею про їх проведення у кримінальних провадженнях про використання доходів, здобутих від незаконного обігу наркотиків зазвичай повинні проводитись:

а) в банківських установах, через які «проходили» злочинні кошти, а також в яких відкриті рахунки підприємств, установ, організацій, окремих осіб, котрі приймали участь у використанні злочинних доходів – з метою вилучення документів, що підтверджують зарахування, перерахування та зняття коштів з рахунків, супутніх документів, особових справ клієнтів та ін.;

б) на біржах, в інвестиційних компаніях, комерційних структурах, благодійних організаціях, пов’язаних з операціями по використанню злочинних доходів – з метою вилучення документів;

в) в органах та у осіб, які виконували дії, пов’язані з проведенням і реєстрацією відповідних операцій зі злочинними коштами (нотаріуси, бюро технічної інвентаризації, регіональні сервісні центри МВС України у областях – по питаннях реєстрації автомототранспорту та ін.) – з метою вилучення документів щодо цих операцій;

г) в архівах, якщо у використанні коштів приймали участь суб’єкти господарювання, що ліквідувались і чия документація на момент розслідування здана в архів;

д) у окремих осіб, у яких наявні предмети чи документи (наприклад, у родичів, знайомих підозрюваного), що мають значення для досудового розслідування – з метою вилучення таких предметів і документів, які мають

відношення до провадження (наприклад, документів, що підтверджують право власності на нерухомість, цінних речей тощо).

У ст. 30 Конституції України визначено, що проникнення в житло або в інше володіння особи, для проведення обшуку, можливе лише за вмотивованим рішенням суду. Згідно зі статтями 234, 235, 236 чинного КПК України обшук проводиться за мотивованою ухвалою слідчого судді. Зважаючи на специфіку обшуку, закон дозволяє слідчому у невідкладних випадках, проводити його без постановлення ухвали слідчого судді, але з обов'язковим повідомленням прокурора і слідчого судді про проведений обшук протягом доби. Так, без ухвали слідчого судді, обшук житла або іншого володіння особи може бути проведений у невідкладних випадках, пов'язаних з врятуванням життя та майна чи з переслідуванням осіб, підозрюваних у вчиненні злочину. В цьому випадку у протоколі вказують причини, які обумовили проведення обшуку без постанови судді з направленням прокурору протягом доби копії протоколу.

У разі проведення тимчасового доступу до речей та документів в банківських установах, правоохоронні органи повинні керуватися ще й Законом України від 07.12. 2000 року № 2121-III «Про банки і банківську діяльність». Згідно з п. 2 та п. 3 ч. 1 ст. 62 Закону України «Про банки і банківську діяльність», інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками за рішенням суду. Органам прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу.

Слідчий повинен знати, що згідно ст. 60 Закону України «Про банки і банківську діяльність» від 07.12.2000, *банківською таємницею* є інформація, щодо діяльності та фінансового стану клієнта, яка стала відома банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банком і розголошення якої може завдати матеріальної чи

моральної шкоди клієнту. Крім того, банківську таємницю становить інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду.

Отже, банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації.

У випадках, коли при розслідуванні кримінального провадження, необхідна вказана інформація, вона надається: а) за рішенням суду; б) органам прокуратури України, Служби безпеки України, Державному бюро розслідувань, Національної поліції, Національному антикорупційному бюро України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу – на їх письмову вимогу. Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, відповідно до ст. 62 Закону України «Про банки і банківську діяльність» повинна:

1) бути викладена на бланку державного органу встановленої форми або надіслана в електронному вигляді;

2) бути надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою, або бути завіреною

кваліфікованим електронним підписом керівника державного органу (чи його заступника);

3) містити передбачені цим Законом підстави для отримання цієї інформації;

4) містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Крім того, при розслідуванні злочинів передбачених ст. 306 КК України кошти або інформація щодо них, здобуті від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів можуть пересилатися також через поштове відділення зв'язку України. В цьому випадку слідчий за погодженням з прокурором зобов'язаний звернутися до слідчого судді з клопотанням про дозвіл на втручання у приватне спілкування, в порядку передбаченому ст.246, 248, 249 КПК України. Одним із видів втручання в приватне спілкування є арешт, огляд і виїмка кореспонденції.

Накладення арешту на кореспонденцію, її огляд і виїмка можуть бути застосовані лише за наявності достатніх підстав вважати, що поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб їй може містити відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування, і іншими способами одержати ці дані неможливо.

Накладення арешту на кореспонденцію полягає в забороні установам зв'язку та фінансовим установам вручення кореспонденції адресату без відповідної вказівки слідчого, прокурора. Затримавши відправлення, яке відповідає встановленим ознакам, співробітник поштової установи повідомляє про це слідчого або відповідного працівника уповноваженого оперативного підрозділу, якому доручено здійснювати НСРД.

Огляд і виїмка кореспонденції (ст. 262 КПК) полягає в негласному відкритті й огляді затриманої кореспонденції, на яку накладено арешт, її виїмці або знятті копії чи отриманні зразків, нанесенні на виявлені речі і документи спеціальних позначок, обладнанні їх технічними засобами контролю, заміні

речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги. Огляд кореспонденції проводиться слідчим в установі зв'язку, якій доручено здійснювати контроль і затримувати цю кореспонденцію, за участю представника цієї установи, а за необхідності – за участю спеціаліста. За результатами огляду та його наслідками складається протокол згідно з вимогами статей 104-107, 252 КПК.

3.4. Особливості проведення допиту при розслідуванні злочинів передбачених ст. 306 КК України

У якості свідків по кримінальним провадженням щодо використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів допитують наступних осіб:

1. Осіб, які приймали участь у вчиненні первинних злочинів у сфері наркобізнесу, але не є співучасниками використання здобутих злочинним шляхом доходів. Ці особи можуть бути допитані як свідки лише у випадках, коли кримінальне провадження про первинний злочин розслідується окремо від провадження про використання «брудних» коштів. В інших випадках вони допитуються відповідно до свого статусу у кримінальному провадженні (підозрюваний) про первинний злочин.

2. Працівників банків, через які «проходили» злочинні кошти. У цих свідків слід з'ясовувати: а) обставини відкриття рахунків установами чи особами, причетними до злочину; б) обставини здійснення операцій по їх рахунках; в) відомості про осіб, які звертались до банку в ході цих операцій; в) чи мали місце відхилення від звичайного порядку здійснення банківських операцій при обслуговуванні цих клієнтів, якщо так, то які, хто їх припустив, з яких причин; г) інші обставини, що мають значення для досудового розслідування.

3. Працівників установ зв'язку, через які «проходили» злочинні кошти або інформація щодо цих коштів (у поштово-телеграфній кореспонденції) у

випадку, якщо було проведено негласну слідчу (розшукову) дію – накладення арешту на кореспонденцію, її огляд і виїмка. Також понятих з числа працівників установи зв'язку, які були присутні під час проведення огляду та виїмки поштово-телеграфної кореспонденції, на яку було накладено арешт.

4. Осіб, які приймали участь при підготовці, укладенні та реєстрації правочинів, що, як потім з'ясувалось, здійснені з метою використання злочинних доходів (працівники державних органів, нотаріальних контор, БТІ, агентств з нерухомості та ін.). У цих осіб слід одержувати показання про обставини вказаних операцій.

5. Осіб, які мають спеціальні знання, з роз'яснення фахових питань.

6. Родичів, близьких знайомих, друзів підозрюваного з обставин злочину, що їм відомі та з питань, що стосуються вивчення особи підозрюваного.

Вказаний перелік не є остаточним, тому слідчий обирає тактику розслідування виходячи із матеріалів конкретного кримінального провадження і обставин вчиненого злочину.

СЛОВНИК ТЕРМІНІВ, ЩО ВИКОРИСТОВУЮТЬСЯ В МЕРЕЖІ ІНТЕРНЕТ

ADSL (Asymmetrical Digital Subscriber Line) – асиметрична цифрова абонентська лінія.

ASCII (American Standard Code for Information Interchange) – американський стандартний код для обміну інформацією.

ASCIIZ – рядок символів коду ASCII, що закінчується символом NULL.

BIOS (Basic Input/Output System) – базова система може вводу\виводу

BISDN (Broadband ISDN) – широкосмугова цифрова мережа інтегрованих послуг.

CDMA (Code Division Multiple Access) – множинний доступ з кодовим розділянням (каналів).

CDROM (Compact Disk RcadOnly Memory) – постійна пам'ять на компактдиску; постійний запам'ятовувальний пристрій на компактдиску; компактдиск, який не можна перезаписати.

CDROM XA, CDROM/XA (Compact Disk Read Only Memory cXtcnded Architecture) – компактдиск, який не можна перезаписати, з розширеною архітектурою; нестирання пам'яті, на компактдиску з розширеною архітектурою.

DB (DataBase) – базові дані, база даних.

Dbkey (DataBase KEY) – ключ бази даних.

DBS (Digital Banking System) – цифрова банківська система.

DDD (Direct Distance Dialing) – автоматичний виклик віддаленого абонента.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налагоджування конфіїгурації головної ЕОМ.

DNS 1. (Domain Name System) доменна (доменова) – система імен.

DNS 2. (Domain Name System (Service)) – система (служба) іменування доменів (протокол обслуговування каталогів у TCP/IP).

DRAM (Dynamic Random Access Memory) – динамічна оперативна пам'ять.

DRAW (Direct Read After Write) – безпосереднє читання після записування (контроль запису на оптичний диск); читання безпосередньо після записування.

DRCS (Dynamically Redefinable Character Set) – динамічно завантажувані шрифти.

DSN (Digital Switching Network) – цифрова комунікаційна мережа.

EACC (ErrorAdaptive Control Computer) – стійка до помилок керівна ЕОМ.

EBCS (Electronic Business Communication System) – система передавання ділової інформації.

ETC (Enhanced Throughput Cellular) – удосконалений стільниковий зв'язок (протокол корпорації AT&T для виправляння помилок передавання в стільникових мережах).

FA (Final Address (register)) – регістр кінцевої адреси. **FAQ (Frequently Asked Questions)** – часто задавані запитання.

FAT (File Allocation Table) – таблиця розміщення файлів (в операційній системі ДОС).

FTP 1. (File Transfer Program) – програма передавання файлів.

FTP 2. (File Transfer Protocol) – протокол передавання файлів.

FTU (FirstTime User) – новий користувач.

GEOS (Geostationary EarthOrbiting Satellite) – геостаціонарний супутник.

GIF (Graphic Interchange Format) – формат для обміну графічною інформацією; формат обміну графічними даними.

GM (Global Memory) – глобальна пам'ять.

HDD (Hard Disk Drive) – дисковод жорсткого диска, вінчестер.

HS (HighSpeed) – швидкопрохідний, швидкісний.

IBMcompatible – IBMсумісний.

IR 1. (Information Retrieval) – пошук інформації, інформаційний пошук.

IR 2. (InfraRed) – інфрачервоний.

IR 3. (Instruction Register) – регістр команд.

IR 4. (Internal Resistance) – внутрішній опір.

IR 5. (InterrogatorResponder) – запитувачвідповідач.

IR 6. (Interrupt Register) – регістр переривань.

ISDN (Integrated Services Digital Network) – цифрова мережа інтегрованих послуг; цифрова мережа зв'язку з інтеграцією служб і комплексними послугами.

JPEG (Joint Photographies Expert Group) – спеціальний графічний формат, який розробила об'єднана група експертів з фотографії. Дає змогу зберігати картинки у файлах найменших розмірів.

LBA (LinearBounded Automaton) – автомат з лінійно обмеженою пам'яттю.

LBN (Logical Block Number) – номер логічного блоку.

LPT (Line PrinTer) – паралельний порт для принтера.

MAC 1. (MachineAided Cognition) – навчання за допомогою (обчислювальної) машини.

MAC 2. (MACintosh) – серія персональних комп'ютерів (комп'ютерів) фірми Apple.

MAC 3. (Maximum Allowable Concentration) – максимально допустима концентрація.

MAC 4. (Medium Access Control) – керування доступом до середовища (даних).

MAC 5. (Message Authentication Code) – код підтвердження автентичності повідомлення.

MAC 6. (MicroprocessorArray Computer) – обчислювальна машина на основі матриці мікропроцесорів.

MBR (Master Boot Record) – первинний завантажувач диска. **MODEM (MOdulator/DEModulator)** – модулятордемодулятор, модем.

NETACP (NETwork Ancillary Process) – процес допоміжного керування мережею.

NETBEUI (NETBIOS End User Interface) – інтерфейс кінцевого користувача з NETBIOS.

NETBIOS (NETwork Basic Input/Output System) – мережева базова система вводу\виводу.

NT 1. (Nested Task) – вкладена задача.

NT 2. (Network Terminal) – мережевий термінал.

NT 3. (New Technology) – нова технологія.

NT 4. (No Transmission) – немає передавання.

NVROM (NonVolatile ReadOnly Memory) – снергонезалежна постійна пам'ять.

PDB 1. (Physical Data Base) – фізична база даних.

PDB 2. (Populated DataBase) – заповнена база даних.

PDB 3. (Process DataBase) – база даних про процеси.

PDB 4. (Protected DataBase) – захищена база даних.

PDBR (Page DirecloryBase Register) – базовий регістр ката
логу сторінок.

PDF 1. (Portable Data File) – компактний файл даних.

PDF 2. (Portable Document Format) – переносний формат документів.

POSI (Portable Operating System Interface) – переносимий інтерфейс для операційних систем.

RAM (Random Access Memory) – запам'ятовувальний пристрій з довільним вибиранням, робоча (оперативна) пам'ять.

RIP (Raster Image Processor) – процесор растрових зображень; растровий процесор.

RISC 1. (Reduced Instruction Set Computer) – комп'ютер зі скороченим набором команд.

RISC 2. (Reduced Instruction Set Computing) – спрощена система машинних команд.

ROM (ReadOnly Memory) – постійна пам'ять, постійний запам'ятовувальний пристрій, пам'ять тільки для читання.

SMTP (Simple Mail Transfer Protocol) – простий протокол пересилання (передавання) пошти. Стандартний протокол Internet для передавання повідомлень електронної пошти між комп'ютерами.

SNAP (Standard Network Access Protocol) – стандартний протокол мережевого доступу.

STD (Subscriber Trunk Dialing) – набирання номера для міжміського зв'язку.

SYS (SYStem library) – системна бібліотека.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол керування передаванням (міжмережевин протокол). Набір протоколів, які керують Internet і визначають способи передавання даних між комп'ютерами.

TCSEC (Trusted Computer System Evaluation Criteria) – критерії оцінювання придатності комп'ютерних (компуторних) систем.

TXT (TeXT) – текст.

UFD (User File Directory) – каталог файлів користувача.

UFI (User Friendly Interface) – дружній інтерфейс.

VBF (Variablelength Bit Field) – бітове поле змінної довжини. **WIN (Wireless Inbuilding Network)** – безпроводова внутрішня мережа.

WRU (Who aRc yoU) – «хто ви?» (сигнал запиту).

WTH (What The Heck) – «якого чорта!».

WWW (WorldWide Web) – «всесвітня павутина». Система, яка використовує для переходів між джерелами даних гіпертекстові посилання, а це дає змогу одержувати доступ до мережевих ресурсів з різних точок входу.

WYDIWYS (What You Do Is What You See) – «що зробиш, те й побачиш"» (на екрані дисплея).

WYPIWYF (What You Print Is What You Fax) – «що надрукуєш, те й буде передано по факсу».

WYSIWYG (What You Sec Is What You Get) – «що бачиш, те й маєш» (зображення на екрані еквівалентне надрукованому); режим повної візуальної відповідності: що побачиш на екрані, те й одержиш друком.

Адміністратор (administrator) – це власник сайту, особа, яка має найбільші повноваження.

Анімація (animation) – це один із способів подання рухомих зображень у мережі Інтернет.

Байт (byte) – це основна одиниця виміру кількості інформації, що дорівнює 8 Біт.

Банер (banner) – це графічний об'єкт, який рекламує певний сайт або продукцію.

Біт – це найменша одиниця виміру кількості інформації.

Браузер (browser) – це клієнтська програма для роботи у Всесвітній Павутині , яка дозволяє користувачу переглядати зміст webсторінок.

Гіперпосилання (hyperlink) – це слово чи зображення в електронному документі, що містять посилання на інші файли.

Гіпертекст (hypertext) – це електронний текст, що містить у своїй структурі посилання на адреси інших файлів.

Головна сторінка (home page) – це початкова (титульна) сторінка webсайта.

Дизайн (design) – зовнішній вигляд чогось: сайту, логотипу, листівки...

Домен, доменне ім'я (domen) – це літерне (літерноцифрове) позначення сайту, тобто його ім'я.

Електронна пошта (Electronic Mail, Email) – це канал передачі текстових повідомлень і вкладених файлів між двома підключеними до Інтернету комп'ютерами.

Інтернет (Internet) – це складна електронна інформаційна структура, що представляє собою глобальну мережу, яка може пов'язувати між собою комп'ютери, розташовані в будь-якій точці Земної кулі і здійснювати між ними обмін інформацією.

Інтернет магазин – це складна автоматизована електронна система, призначена для реалізації товарів і послуг комерційних підприємств із застосуванням мережевих технологій.

Інтернетсторінка – це документ особливої структури, створений спеціально для перегляду в Інтернеті.

Кеш (cache) – це системна папка, в яку комп'ютер записує всі документи, отримані користувачем з мережі.

Клік (click) – це натиснення на якийсь об'єкт на інтернет сторінці, що містить посилання на картинку, банер, текст.

Контент (content) – це зміст. Під даним терміном частіше усього розуміється змістовне наповнення електронних ресурсів, наприклад, webсайтів.

Партнерська програма – це спеціальна схема отримання фінансового прибутку в Інтернеті, відповідно до якої учаснику платять за кожного унікального відвідувача, що прийшов на сайт рекламодавця з рекламного банера, розміщеного на сторінці учасника.

Підтримка web–сайту – це спеціальний комплекс процедур, що забезпечують працездатність ресурсу Інтернету.

Портал (portal) – це Інтернет–сайт, що надає максимально широкий спектр послуг, які відповідають потребам середньостатистичного користувача мережі.

Просування сайту – це дії, спрямовані на залучення відвідувачів на сайт і на просування його до вершин пошукових систем.

Розсилка – це розсилання багатьом користувачам певної інформації, яка їх зацікавить.

Рунет – це російський Інтернет, тобто всі сайти перебувають на російській зоні Інтернету.

Сайт (site) – це сукупність логічно зв'язаних webсторінок, розміщених, як правило, на одному комп'ютері.

Сервер (server) – це комп'ютер, який надає свої ресурси іншим комп'ютерам мережі, або програма, що обслуговує запити на доступ до ресурсів свого комп'ютера.

Серфінг (serfing) – це перегляд Інтернет сторінок.

Спам (spam) – це незаконне розсилання листів, оголошень без погодження з власником поштової скриньки чи сайту.

Трафік (traffic) – 1. Потік повідомлень або об'єм переданої інформації. 2. Кількість відвідувачів webсайту або будь-якої його сторінки за одиницю часу (день, місяць, рік).

Форум (forum) – це такий модуль для спілкування, де можна створювати теми, задавати питання і чекати від інших користувачів відповідей.

Хіт (від англ. hit – натиснення) – це одне відвідування будь-якої сторінки webсайту.

Хост – це будь-який підключений до Інтернету комп'ютер, незалежно від його призначення.

Хостинг (hosting) – це послуга виділення місця на сервері для розміщення свого сайту.

Чат (chat) – це модуль для спілкування в реальному часі. Може бути у вигляді програмного забезпечення, або Інтернет сайту.

Література:

1. Інструкція з організації проведення та оформлення експертних проваджень у підрозділах судових експертиз і експертних досліджень у підрозділах Експертної служби Міністерства внутрішніх справ України : затверджена наказом МВС України від 17.07.2017 № 591, зареєстрована наказом Міністерства юстиції України від 18.08.2017 № 1024/30892 // База даних «*Законодавство України*». Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/z1024-17.
2. Про затвердження Положення про Департамент протидії наркозлочинності Національної поліції України : наказ Національної поліції України від 17.11.2015 № 95.
3. Про затвердження Положення про Департамент кіберполіції Національної поліції України : наказ Національної поліції України від 10.11.2016.
4. Про затвердження Положення про Департамент захисту економіки Національної поліції України : наказ Національної поліції України від 1 (службу скасовано).
5. Про стимулювання ринку криптовалют та їх похідних в Україні: проект Закону № 7183-1 від 10.10.2017 // База даних «Законодавство України» / Верховна рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=62710&pf35401=4360
6. Роз'яснення щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin // Національний банк України. 10.11.2014. URL: https://www.bank.gov.ua/control/uk/publish/article?art_id=11879608
7. Особливості розслідування незаконного виробництва, виготовлення, придбання, зберігання, перевезення, пересилання чи збуту наркотичних засобів, психотропних речовин або їх аналогів: Методичні рекомендації для практичних підрозділів Національної поліції України // В.О. Малярова, С. П. Лапта, С. М. Лозова, Т. П. Матюшкова та ін. / за заг. редакцією к.ю.н. Кікінчука В. В. Х. : ХНУВС, 2017. 76 с.
8. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореферат дис. на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Харківський національний університет внутрішніх справ. Харків. 2017. 19 с.
9. Особливості досудового розслідування незаконного виробництва, виготовлення, придбання, зберігання, перевезення, пересилання чи збуту наркотичних засобів, психотропних речовин або їх аналогів в умовах нового кримінального процесуального та оперативно-розшукового законодавства : наук.-метод. реком. // К. Л. Бугайчук, О. О. Савченко, Н. О. Прибиткова. Харків. ХНУВС. 2015. 99 с.
10. 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, М. Стрільців, В. Б. Школьний та ін. К. : ГСУ МВС України, Нац. акад. внутр. справ, 2012. 30 с.
11. Идеальная площадка. Торговля наркотиками быстро переходит в Интернет. *Корреспондент.net*. 15 квітня 2015, 11:02. URL: http://korrespondent.net/ukraine/events/3503719-ydealnaia-ploschadka-torhovlia-narkotykamy-bystro-perekhodyt-v-ynternet.
12. Наркоторговцы занимались майнингом криптовалюты в Украине // Delo.ua. 22 січня 2018, 21:01. URL: https://delo.ua/ econonomyandpoliticsinukraine/narkotorgovcy-zanimalis-majningom-kriptovaljuty-338232/.
13. Гладкова Е.О. Стратегія й тактика протидії наркозлочинності в Україні. : монографія. Харків. Панов. 2019. 416 с.
14. Юхно О.О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник*

Харквського національного університету внутрішніх справ. 2016. № 2 (76). Харків. ХНУВС. С. 86-95.

15. Лазарєв А.П. Слідчі (розшукові) дії у кримінальному провадженні : теорія та механізм реалізації : монографія. Харків. ФОП Панов А.М. 2019. 212 с.

16. Туманов С.Г. Арешт та вилучення майна в кримінальному провадженні та інші пов'язані питання : зб. норм. актів та судової практики. Харків. Право. 2020. 416 с.

17. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. URL: http://www.cyberpol.ru/cybercrime.shtml

18. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824IV (282415) від 07.09.2005, ВВР, 2006, N 56, ст. 71.

19. Уголовный кодекс Российской Федерации / Авт.сост. Коммент. Д. А. Гайдуков, С. А. Перчаткина. – М. : Эксмо, 2009.– 336 с.

20. Уголовный кодекс Республики Польша / Науч. ред. А. И. Лукашова, Н. Ф. Кузнецовой; Пер. с польск. Д. А. Барилович. – СПб. : Юридический центр Пресс, 2001. – 234 с.

21. Кримінальний кодекс України за станом на 05.07.2012 року. *Відомості Верховної Ради України*. 2001 (зі змінами на 17 серпня 2020 р.).

22. Уголовный кодекс Федеративной Республики Германии / Науч. ред. и вступ. статья Д. А. Шестакова; предисл. доктора права Г. Г. Йешека; перевод с нем. Н. С. Рачковой. – СПб. : Юридический центр Пресс, 2003. – 524 с.

23. 15й, 17й, 18й, 42й, 47й зводи законів США // Современное право средств массовой информации в США. М. 2000. С. 205-223.

24. Розділ статистичних досліджень організації Nua Internet Surveys [Електронний ресурс]. URL: http://www.virtualref.com/subj/101.ht

25. Закон України «Про основи національної безпеки України» зі змінами та доповненнями *Відомості Верховної Ради України* (ВВР), 2003, N 39, ст. 351.

26. Гуславский В. С., Задорожний Ю. А., Розовский В. Г. Информационноаналитическое обеспечение раскрытия и расследования преступления: монография Луганск. ТОВ «Елтон2», 2008. 133 с.

27. Соціальна мережа «Facebook» [Електронний ресурс]. URL: http://www.facebook.com

28. Соціальна мережа «Instagram» [Електронний ресурс]. URL: http://www. Instagram.com

29. Цехан Д. М. Використання високих інформаційних технологій в оперативнорозшуковій діяльності органів внутрішніх справ: монографія. За науковою редакцією О. О. Подобного. Одеса : Юридична література, 2011. 216 с.

30. Пошуковий сервіс «Google» [Електронний ресурс]. URL: http://www.google.com

31. Пошуковий сервіс «МЕТА» [Електронний ресурс]. URL: http://www.meta.ua

32. Пошуковий сервіс «Yahoo!» [Електронний ресурс]. URL: http://www.yahoo.com

33. Пошуковий сервіс «Bing» [Електронний ресурс]. URL: http://www.bing.com

34. Пошукові оператори «Google» [Електронний ресурс]. URL: http://www.googleguide.com/advanced_operators.html

35. Как надо использовать язык поисковых запросов «Google» [Електронний ресурс]. – Режим доступу: http://www.diacr.ru/zametki/20kakpravilnoiskatvgoogle/kakpravilnoiskatvgoogle.htmРасширенные возможности поиска в «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.gmail.com/ search/?id=481920Сервіс пошуку файлів на FTPсерверах «FileSearch» [Електронний ресурс]. – Режим доступу: http://www.filesearch.com

36. Сервіс пошуку файлів на FTPсерверах «МАМОНТ» [Електронний ресурс]. – Режим доступу: http://www.mm

37. Менеджер завантажень файлів «Download Master» [Елек тронний ресурс]. – Режим доступу: http://www.westbyteПошуковий сервіс «Google Images» [Електронний ресурс]. – Режим доступу: https://www.google.com.uaПошуковий сервіс графічних зображень «TinEye Reverse Image Search» [Електронний ресурс]. – Режим доступу: http://www. tineye.coПошуковий сервіс графічних зображень «GazoPa similar image search» [Електронний ресурс]. – Режим доступу: http://www.gazopa.com

38. Офіційний сайт «Internet Assigned Numbers Authority» (IANA) [Електронний ресурс]. – Режим доступу: http://www.iana.org

39. Сервіс ідентифікації користувача за IP адресою «WHOIS» Інтернет–ресурсу «2IP.UA» [Електронний ресурс]. – Режим доступу: http://2ip.ua/whois

40. Кримінальний процесуальний кодекс України : станом на 17 серпня 2020. Харків. Право. 2020. 424 с.

41. Єдиний реєстр досудових розслідувань України [Електронний ресурс]. URL: https://erdr.gp.gov.ua

42. Доповнення для загрузочної операційної системи «BartPE», яке дозволяє змінювати чи відключати паролі користувачів в операційних системах [Електронний ресурс]. URL: http://www.kood.org/windowspasswordrenew.

43. Зацеркляний М.М., Наумов В.В. Інформаційні системи і технології в діяльності правоохоронних органів: навч.посіб. Харків: Тимченко. 2010. 382 с.

44. Афанасьев В. Г. Социальная информация и управление обществом. Москва. Политиздат, 1975. 408 с.

45. Венгеров А. Б. Категория «информация» в понятийном аппарате юридической науки. *Советское государство и право*. 1977. № 10. С. 7078.

46. Кудрявцев Ю. В. Ценность правовой информации.

47. Известия высш. учеб. заведений. 1977. № 1. С. 4551. (Сер. : Правоведение).

48. Информация и оперативнорозыскная деятельность : монография / А. С. Овчинский ; [под ред. В. И. Попова]. Москва: ИНРФАМ, 2002. 97 с.

49. Горбачов А. Електронна інформація як доказ при розслідуванні злочинів у сфері комп'ютерних технологі. *Компьютерная преступность и кибертерроризм* : сб. науч. ст. Запорожье, 2005. Вып. 3. С. 157.

50. Айламазян А. К., Е.В. Стась Информатика и теория развития. Москва. Наука. 1989. С. 31.

51. Головчик В. Я. Історія ОРД «*Актуальні проблеми сучасної науки і правоохоронної діяльності*»: матеріали XI науковопрактичної конференції курсантів та слухачів, 29 травня 2004 р. Харків: Вид-во Національного університету внутр. справ. 2004. 276 с.

52. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений. *Вісник ЛДУВС*. 2010. № 1, спец. вип. № 2. С. 314.

53. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. Київ. Юрінком Інтер, 2012. 608 с.

54. «Про оперативно-розшукову діяльність» [Електронний ресурс] : закон України від 18.01.2006 р. № 2135XI1 в редакції Закону України від 01.01.2011 р. № 275617. – Електрон, дан. (1 файл). URL: http://zakon1.rada.gov.ua.

55. Жукова Е. А. HiTech : феномен, функции, формы / Е. А. Жукова ; [под ред. И. В. МеликГайказян]. Томск : ТГПУ. 2007. 367 с.

56. Румянцева Е. Л. Информационные технологии : учеб. пособ. / Е. Л. Румянцева, В. В. Слюсарь; [под. ред. Л. Г. Гагариной].- М.: Форум : ИнфраМ, 2007. С. 15.

57. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційнопошукових систем для забезпечення проведення негласних слідчих (розшукових) дій. *Право і Безпека* : науковий журнал. № 4 (46) за 2012 рік. Харківський національний університет внутрішніх справ : видавництво ХНУВС. 2012. 360 с.

58. Таненбаум Э. Архитектура компьютера. 5е изд. (+CD). СПб.: Питер, 2007. 844 с.

59. Организация ЭВМ. 5е изд. / К Хдоэхор. 3. Вранешич. С. Зэки. СПб. Питер; Киев. Издательская группа BHV. 2003. 848 с.: ил. (Серия «Классика computer science»).

60. Кримінологія. (Загальна частина): Підручник / Кол. авторів Блага А. Б., Богатирьов І. Г., Давиденко Л. М. та ін.; за заг. ред. О.М. Бандурки. Харків: Видво ХНУВС. 2010. 280 с.

61. Кримінальний кодекс України (із змінами та доповненнями на 1 липня 2020 року). Харків. Одіссей. 2020. 232 с.

62. Захарченко В.Ю., Лазуренко В. И., Олифиров А.В., Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: учебное пособие / Под общ. редакцией В. И. Лазуренко. Київ. Центр учебной литературы, 2007. 170 с.

63. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс]. / Комітет протидії корупції та організованої злочинності. – Режим доступу: http://kpk.org.ua/2007/02/05/ kberzlochinnst_v_ukran_perspektivi_protid.html.

64. Словарь криминологических и статистических терминов / А. Г. Кальман, И. А. Христич. Харків. Гимназия : Инт изучения проблем преступности АПрН Украины, 2001. 94 с.

65. Категорія: кіберзлочинність. [Електронний ресурс]. URL: http://uk.wikipedia.org/wiki/ категорія: кіберзлочинність.

66. Компьютерные преступления их предупреждение и выявление : учеб. пособие. Київ : Центр учеб. лит., 2007. 170 с.

67. Голубєв, В. Суб'єкт злочинної діяльності у сфері використання електроннообчислювальних машин. *Підприємництво, господарство і право* . 2004 . № 6. С. 109-112.

68. Типология и классификация в социологических исследованиях. / В. Г. Андреенков, Ю. Н. Толстова; Институт социологических исследований (Академия наук СССР) – М, 1982. – 295 с.

69. Голубев В. А., Головин А. Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий. [Электронный ресурс]. – Режим доступа: www.crime– research.ru.

70. Голубев В. О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя. 2003. С. 82-92.

71. Комп'ютерна злочинність: навч. посібник. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. Київ. 2002. 240 с.

72. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государствчленов, международного сообщества и частного сектора // Группа экспертов для проведения всестороннего исследования киберпреступности Вена, 25–28 февраля 2013 года : [Электронный ресурс] / UNODC/CCPCJ/EG. 2013. 21 с.URL: http://www.unodc.org/documents/organized.
crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_ 2_R.pdf

73. Конвенція про кіберзлочинність від 23 листоп. 2001 р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.

74. 71. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Науковий журнал *Право і Безпека*. 2011. №4. [Електронний ресурс]. URL: http://archive.nbuv.gov.ua/portal/soc_gum/pib/ 2011_4/PB–4/PB–4_26.pdf

75. Селико Ю., Прохоров А. Internet – отмычка для компьютера. Комп’ютерпресс. 2002. №3. С. 40–43.

76. Бутузов В.М. До питання специфіки протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика*). 2008. № 18. С. 38-47.

77. Про ратифікацію Конвенції про кіберзлочинність : закон України від 7 верес. 2005 р. № 2824IV. *Відомості Верховної Ради України*. 2006. №56.Ст. 71.

78. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні

системи [Електронний ресурс]. URL: http://www. zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?=nreg=994_687.

79. Одиннадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. URL: http://www.un.org/russian/events/ 11thcongress/ index.html.

80. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. URL: http://www.un.org/ru/conf/crimecongress2010.

81. Агентства ООН объединились против киберпреступности [Электронный ресурс]. URL: http://www.unmultimedia.org/radio/russian/detail/84626.html.

82. Стратегія національної безпеки України [Електронний ресурс] : указ Президента України від 12 лют. 2007 р. № 105/2007. URL: http://zakon1.rada.gov.ua/ laws/show/105/2007.

83. Вехов В. Б. Компьютерные преступления, способы совершения методики расследования. Москва. 1996. 182с.

84. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229/99 [Електронний ресурс]. URL: http://zakon2.rada.gov.ua/laws/show/1229/99.

85. 83. Юхно О.О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник Харківського національног*о *університету внутрішніх справ*. 2016. № 2 (76). Харків. ХНУВС. С.8695.

86. 84.Топчій В.В. Кримінально-правові та кримінологічні заходи запобігання злочинам у сфері інтелектуальної власності в Україні : монографія. Ірпінь. Університет ДФС України. 2019. С. 408 с.

87. 85. Александр Загуменный, Александр Юхно Использование современных телекоммуникационных и других технологий при проведении следственных действий. Международный научно-практический журнал *Закон и Жизнь.* 2020. № 67 (342-343) июнь-июль. С. 79-84.

88. 86. Юхно .О. О., Загуменний Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних (слідчих) розшукових дій : нав.посіб. Видання друге, доп. і перероб. (Серія «Бібліотека слідчого і детектива : проблеми кримінального процесу»). Харків. Колегіум. 2020. 116 с.

89. 87. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. За заг. ред. А.Ф. Волобуєва. Одеса. Тес. 2020. 372 с.

Нормативні-правові акти, що застосовуються як бланкетні норми при застосуванні статті 306 КК України

1. Конвенція про боротьбу проти незаконного обігу наркотичних засобів та психотропних речовин 1988 р., ратифікована Україною 25.04.1991.

2. Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, від 08.11.1990, ратифікована Україною 17.12.1997.

3. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» в редакції від 16.08.2020 (Відомості Верховної Ради України (ВВР), 2020, № 25, ст.171)

4. Закон України «Про внесення змін до деяких законів України з питань запобігання використання банків та інших фінансових установ з метою легалізації (відмиванню) доходів, одержаних злочинним шляхом» від 06.02.2003 № 485-IV.

5. Сорок рекомендацій Групи з розробки фінансових засобів боротьби з відмиванням грошей (FATF) в редакції від 24.09.2003.

6. Постанова Пленуму Верховного Суду України від 15.04.2005 № 5 «Про практику застосування судами законодавства про кримінальну відповідальність за легалізацію (відмивання) доходів, одержаних злочинним шляхом».

1. Закон України «Про наркотичні засоби, психотропні речовини і прекурсори» від 15.02.1995 № 60/95-ВР в редакції від 05.07.2020.

2. Закон України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними» від 15.02.1995 № 62/95-ВР в редакції від 03.07.2020.

3. Постанова Кабінету Міністрів України від 06.05.2000 № 770 «Про затвердження переліку наркотичних засобів, психотропних речовин і прекурсорів» поточна редакція від 17.09.2020.

4. Постанова Пленуму Верховного суду України від 26.04.2002 № 4 «Про судову практику в справах про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів» (із змінами, внесеними згідно з Постановою Верховного Суду від 18.12.2009 № 16).

Наукове видання

Юхно Олександр Олександрович
Коршенко Вадим Анатолійович
Гнусов Юрій Валерійович
Носов Віталій Вікторович
Матюшкова Тетяна Петрівна
Заворіна Олена Петрівна
Лисенко Андрій Миколайович
Загуменний Олександр Олександрович
Туренко Дар'я Вікторівна

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ ОБІГОМ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН, ЇХ АНАЛОГІВ, ПРЕКУРСОРІВ, ОТРУЙНИХ, СИЛЬНОДІЮЧИХ РЕЧОВИН, ОТРУЙНИХ СИЛЬНОДІЮЧИХ ЛІКАРСЬКИХ ЗАСОБІВ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНШИХ ТЕХНОЛОГІЙ

Науково-методичні рекомендації
(на замовлення Головного слідчого управління
Національної поліції України)

За заг. ред. доктора юридичних наук, професора Юхна О.О.

Серія «Бібліотека слідчого і детектива: проблеми кримінального процесу»

Підп. до друку 16.11.2020. Формат 60×84/16.
Ум. друк. арк. 8,4. Обл.-вид. арк. 8,5. Тир. 300 пр. Зам. № 2020-19.
Видавець і виготовлювач – Видавництво «Константа» Україна,
Харківська область, м. Харків, вул. Космічна, 26
Свідоцтво суб'єкта видавничої справи ДК №376 від 22.01.2001