УДК 343.98(477)

О. О. Юхно

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ТА ЇХ ПРОЦЕСУАЛЬНЕ ОФОРМЛЕННЯ

Розглянуто особливості використання сучасних інформаційних технологій під час проведення негласних слідчих (розшукових) дій, форми їх процесуального оформлення та закріплення як доказів у кримінальному провадженні. Описано види негласних слідчих (розшукових) дій згідно з чинним КПК України та проаналізовано можливості їх застосування у правозастосовній діяльності. Запропоновано авторську класифікацію сучасних інформаційних технологій. Проаналізовано думки вчених щодо порушених у статті питань, надано авторську їх оцінку. Зроблено висновок про наявність певних неузгодженостей та неповноти окремих положень чинного КПК України.

Ключові слова: досудове розслідування, кримінальне провадження, сучасні інформаційні технології, негласні слідчі (розшукові) дії, слідчий, оперативний працівник, Інтернет, сучасні технічні засоби та пристрої, обчислювальна техніка, програмне забезпечення.

Постановка проблеми. Наказом Національної поліції України від 10.11.2015 № 85 затверджено Положення про Департамент кіберполіції Національної поліції України, згідно з яким навчається нова категорія поліцейських, формуються центральні та регіональні підрозділи, що матимуть лише вертикальне підпорядкування. Недостатньою є й практика узагальнення щодо застосування негласних слідчих (розшукових) дій, не вирішеними залишаються проблемні питання процесуального закріплення їх результатів, що вимагає дослідження та доопрацювання як її теоретичної частини, так і практичної складової.

Виклад основного матеріалу. Згідно з главою 21 «Негласні слідчі (розшукові) дії» Кримінального процесуального кодексу України [1, с. 327–341] до негласних слідчих (розшукових) дій (далі – НСРД) належать, зокрема, НСРД, пов'язані із втручанням у приватне спілкування. До таких дій кримінальним процесуальним законодавством України віднесено: 1) аудіо-, відеоконтроль особи (ст. 260 КПК України); 2) накладення арешту на кореспонденцію (ст. 261); 3) огляд і виїмка кореспонденції (ст. 262); 4) зняття інформації з транспортних телекомунікаційних мереж (ст. 263); 5) зняття інформації з електронних інформаційних систем (ст. 264). До інших видів НСРД віднесено: 1) обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267); 2) установлення місцезнаходження радіоелектронного засобу (ст. 268); 3) спостереження за особою, річчю або місцем (ст. 269); 4) аудіо-, відеоконтроль місця (ст. 270); 5) контроль за вчиненням злочину (ст. 271); 6) виконання спеціального завдання з розкриття злочинної діяльності організованої групи

чи злочинної організації (ст. 272); 7) негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274).

Необхідно зазначити, що незалежно від різних та інколи протилежних наукових точок зору закріплення в чинному КПК України процесуального інституту негласних слідчих (розшукових) дій все ж таки стало поштовхом для покращення організації, якості, своєчасності розслідування та розкриття злочинів під безпосереднім керівництвом слідчого, прокурора. У зв'язку з ухваленням у 2012 році чинного КПК України як у вчених, так і у правоохоронців та працівників суду виникла велика кількість неузгоджених і проблемних питань у ході наукових досліджень та під час правозастосування положень Кодексу на практиці. Враховуючи велику відповідальність працівників досудового розслідування з указаних питань, слід підтримати наукову позицію Г. Г. Зуйкова, яка полягає в тому, що організацію розслідування слід сприймати як комплекс організаційних методів, засобів та прийомів, які відповідають специфіці злочинів і забезпечують створення оптимальних умов для повного та швидкого розкриття й розслідування злочинів при найбільш раціональній витраті часу, сил і засобів [2]. Крім покращення організації розслідування злочинів, як доречно зазначає Б. Р. Стецюк, з ухваленням нового Кримінального процесуального кодексу України основою кримінального провадження також закріплено змагальність і рівність його учасників, а обсяг процесуальних прав захисту розширено та прирівняно до прав сторони обвинувачення [3, с. 64]. Підтримуючи позиції обох дослідників можемо констатувати, що на підставі вказаного досить суттєво підвищилася і відповідальність щодо дотримання та виконання вимог і положень чинного КПК України, які стосуються діяльності сторони обвинувачення, в тому числі слідчого.

Закріплення в чинному КПК України визначення, підстав проведення та механізму реалізації НСРД – це нова стадія подальшого вдосконалення нормативно-правових актів та службових інструкцій, які регулюють і регламентують здійснення оперативно-розшукової діяльності. Стосовно впровадження у практичну діяльність під час проведення НСРД сучасних технічних засобів, зокрема таких, що базуються на досягненнях інформаційних технологій, на наш погляд, найбільш раціональною є думка Д. М. Цехана [4, с. 71–72]. Він зазначає, що впровадження у практичну оперативно-розшукову діяльність високих інформаційних технологій суттєво модифікувало процес отримання оперативно-розшукової інформації та, як наслідок, спричинило «технізацію» всієї ОРД, а також призвело до: 1) якісної модифікації окремих засобів ОРД; 2) появи нових суб'єктів ОРД (оперативно-технічних підрозділів) та модифікації діяльності інших; 3) того, що техніка стала обов'язковою складовою проведення найефективніших оперативно-розшукових заходів. Означенні процеси, на думку Д. М. Цехана, потребують пошуку нових підходів до організації оперативно-розшукової діяльності в

цілому та використання високих інформаційних технологій в ОРД зокрема [4, с. 71–72], що, на нашу думку, відноситься і до проведення як негласних слідчих (розшукових) дій, так і взагалі слідчих (розшукових) дій.

Крім того, до наукового вивчення та прикладного дослідження проблеми використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуального оформлення безпосередньо спонукає сам чинний КПК України, адже він не містить переліку або визначення тих чи інших технічних засобів, які законодавчо обов'язкові або рекомендовані до використання під час проведення НСРД, та не деталізує окремі аспекти процесуального оформлення за результатами їх проведення. Під час проведення будь-яких негласних слідчих (розшукових) дій на практиці фактично використовуються або технічні пристрої та засоби, або інформаційні технології в тому сенсі, в якому вони пропонуються в цій статті та які викликають ускладнення під час використання, особливо сучасні новітні інформаційні технології у вигляді обчислювальної техніки та програмного забезпечення. Якщо проведення таких НСРД, як аудіо-, відеоконтроль особи чи місця, обстеження публічно недоступних місць, житла чи іншого володіння особи або спостереження за особою, річчю чи місцем не викликає в оперативних підрозділів складнощів, то залежно захищеності каналу передачі даних використання особою, яка кримінально налаштована, спеціального, програмного чи апаратного забезпечення обчислювальної техніки може суттєво ускладнити або унеможливити проведення досудового розслідування. Це, зокрема, стосується таких НСРД, як зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем. Тому виникає необхідність підвищення якості знань працівників поліції у вказаних галузях та інформаційних технологіях.

До першого напряму такої діяльності слід віднести використання сучасних технічних засобів і пристроїв під час проведення негласних слідчих (розшукових) дій, які можуть суттєво покращити ефективність та якісні показники проведення НСРД. Зокрема, це: 1) цифрові дзеркальні наддовгофокусні фото- та відеокамери; 2) відеокамери з режимом зйомки в повній темряві; 3) пристрої нічного бачення; 4) портативні рентгенівські сканери; 5) малі та надмалі пристрої прихованої аудіо- та відеофіксації; 6) сучасні радіосканери. Слід детальніше розглянути НСРД, під час проведення яких доцільно, на нашу думку, використовувати наведені вище сучасні технічні засоби та пристрої наприклад: 1) цифрові наддовгофокусні відеокамери, відеокамери з режимом зйомки у повній темряві, малі та надмалі пристрої скритої аудіо-, відеофіксації доцільно використовувати під час проведення таких НСРД, як: а) аудіо-, відеоконтроль особи (ст. 260 КПК України); б) аудіо-, відеоконтроль місця (ст. 270); 2) цифрові дзеркальні наддовгофокусні фото та відеокамери, відеокамери з

режимом зйомки у повній темряві, пристрої нічного бачення, малі та надмалі пристрої скритої аудіо-, відеофіксації доцільно використовувати під час проведення таких НСРД, як: а) контроль за вчиненням злочину (ст. 271 КПК України); б) спостереження за особою, річчю або місцем (ст. 269); 3) відеокамери з режимом зйомки у повній темряві та пристрої нічного бачення доцільно використовувати під час проведення таких НСРД, як: а) негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК України); б) обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267); 4) сучасні радіосканери доцільно використовувати під час проведення такої НСРД, як установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України); 5) портативні рентгенівські сканери доцільно використовувати під час проведення такої НСРД, як огляд і виїмка кореспонденції (ст. 262 КПК України). Які конкретно технічні засоби необхідно використовувати у вказаних негласних слідчих (розшукових) діях – слід вирішувати слідчому, якщо він проводить їх особисто, чи узгоджувати з працівниками технічних й інших оперативних підрозділів, яким доручено виконувати проведення негласних слідчих (розшукових) дій. Такі знання слід мати для орієнтування щодо можливостей вказаних сучасних технічних досягнень і для запровадження у практичну діяльність.

До другого напряму використання сучасної обчислювальної техніки та програмного забезпечення під час проведення негласних слідчих (розшукових) дій необхідно віднести: 1) обчислювальну техніку у вигляді персональних комп'ютерів, ноутбуків та нетбуків; 2) технічні засоби та пристрої для перехоплення інформації з телекомунікаційних систем; 3) програмне забезпечення для проведення огляду, аналізу та фіксації отриманої інформації. Спираючись на праці таких учених, як О. М. Дубенко [5], О. В. Колпакова [6], В. О. Голубєв [7], Н. С. Постіл і П. В. Цимбал [8], слід класифікувати головні елементи аналітичної комп'ютерної розвідки, що доцільно використовувати у діяльності поліції: 1) фактичний пошук інформації, тобто система дій, яка супроводжується використанням обчислювальної техніки в комплексі із програмним забезпеченням і спрямована на встановлення або підтвердження місця розташування фізичного джерела інформації та виявлення інформації, що представляє доказове значення; 2) фіксація інформації, тобто система дій, спрямованих на збереження отриманої інформації на матеріальних носіях з метою її подальшого використання; 3) аналітична обробка отриманої та збереженої на матеріальних носіях інформації за допомогою логічних прийомів і методів, обчислювальної техніки та програмного забезпечення на основі мети збирання цієї інформації; 4) документальне оформлення результатів обробки отриманої та збереженої на матеріальних носіях інформації.

На нашу думку, викладені елементи аналітичної комп'ютерної розвідки доцільно використовувати для збору та аналізу інформації

під час проведення негласних слідчих (розшукових) дій відповідно до ст. 263 «Зняття інформації з транспортних телекомунікаційних мереж» та ст. 264 КПК України «зняття інформації з електронних інформаційних системи. Така дія є найбільш доцільною та ефективною, ніж будь-яка інша НСРД. Негласна слідча (розшукова) дія «зняття інформації з транспортних телекомунікаційних мереж» регламентована положеннями ст. 263 КПК України, в частині першій якої визначається, що зняття інформації з транспортних телекомунікаційних мереж (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу) є різновидом втручання у приватне спілкування, яке проводиться без відома осіб, які використовують засоби телекомунікації для передавання інформації, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження. Така негласна слідча (розшукова) дія, як «зняття інформації з електронних інформаційних систем», регламентована ст. 264 КПК України, в частині першій якої визначається, що пошук, виявлення та фіксація відомостей, що містяться в електронній інформаційній системі або їх частині, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

Крім того, велике значення з точки зору використання аналітичної комп'ютерної розвідки має положення, яке викладено в ч. 2 ст. 264 КПК України, що не потребує дозволу (ухвали) слідчого судді здобуття відомостей з електронних інформаційних систем або їх частин, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

Під час проведення зазначених вище НСРД щодо цифрової інформації збір і аналіз кількісного та якісного складу інформації, яка передається через телекомунікаційні системи певного комп'ютера, у практичній діяльності можуть бути замінені офіційним вилученням цього комп'ютера та проведенням відносно нього експертизи, оскільки це дозволить отримати інформацію тотожну тій, що перехоплювалась. Однак у такому випадку буде порушено негласність, а для вилучення й тимчасового доступу до комп'ютера будуть необхідні процесуальні підстави, тобто ухвала слідчого судді.

На нашу думку, методи використання широкого спектра наявних на ринку програмного забезпечення та апаратних засобів для перехоплення інформації з телекомунікаційних систем на сьогодні детальніше за всіх виклав у своєму монографічному дослідженні Д. М. Цехан [4, с. 104], який на підставі організаційних варіантів перехоплення поділив їх на: 1) перехоплення засобами оператора

зв'язку; 2) перехоплення власними засобами. Крім того, вчений зазначає, що перехоплення інформації з телекомунікаційних систем може бути реалізовано на різних рівнях: 1) фізичному: а) за допомогою електричних та оптичних роз'єднувачів; б) за допомогою безконтактних датчиків; в) за допомогою перехоплення радіосигналу (для Wi-Fi та інших безпровідних протоколів); 2) канальному рівні: а) за допомогою підключення до концентратора; б) за допомогою функції дзеркалювання порту на комутаторі; в) за допомогою проксування трафіка; г) за допомогою установки сніфера на цільовому або транзитному вузлі; 3) мережевому: а) за допомогою зміни маршрутизації та проксування трафіку; б) за допомогою вбудованих функцій міжмережевого екрана і системи виявлення атак; 4) прикладному: а) за допомогою аналізу трафіка на проксі-сервері; б) за допомогою аналізу трафіка на сервері електронної пошти. Вказана класифікація, на нашу думку, відповідає сучасним вимогам до такого виду інформаційних технологій, який доцільно використовувати у практичній діяльності працівниками поліції, але вона повинна вдосконалюватися разом з удосконаленням інформаційних технологій.

Процесуальне оформлення результатів використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій є кінцевим етапом виконання доручення слідчого працівниками оперативного підрозділу. Вказане потребує процесуального оформлення отриманих результатів згідно з вимогами чинного КПК України для вирішення питання, чи будуть вони визнані доказами.

Для подальшого дослідження порушених питань необхідно враховуватися низку положень чинного КПК України, зокрема: 1) ч. 1 ст. 87 КПК України «Недопустимість доказів, отриманих внаслідок суттєвого порушення прав та свобод людини», у якій зазначено, що недопустимими є докази, отримані внаслідок суттєвого порушення прав і свобод людини, гарантованих Конституцією та законами України, міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок суттєвого порушення прав і свобод людини; 2) ст. 103 КПК України «Форми фіксування кримінального провадження», у якій зазначено, що процесуальні дії під час кримінального провадження можуть фіксуватися в таких формах: а) протокол; б) запис за допомогою технічних засобів; в) журнал судового засідання; 3) ч. 2 ст. 105 КПК України «Додатки до протоколів», у якій зазначено, що додатками до протоколу можуть бути: а) спеціально виготовлені копії, зразки об'єктів, речей і документів; б) письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; в) стенограма, аудіо-, відеозапис процесуальної дії; г) фото-таблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу; 4) ч. 1 ст. 252 КПК України «Фіксація ходу і результатів негласних слідчих (розшукових) дій», у якій зазначено, що фіксація

ходу і результатів негласних слідчих (розшукових) дій повинна відповідати загальним процесуальним правилам фіксації кримінального провадження, положеннями, передбаченим КПК України. За результатами проведення негласної слідчої (розшукової) дії складається протокол, до якого в разі необхідності додаються додатки. Відомості про осіб, які проводили негласні слідчі (розшукові) дії або були залучені до їх проведення, у разі здійснення щодо них заходів безпеки можуть зазначатися із забезпеченням конфіденційності даних про таку особу в порядку, визначеному чинним законодавством; 5) ч. 1 ст. 256 КПК України «Використання результатів негласних слідчих (розшукових) дій у доказуванні», у якій зазначено, що протоколи щодо проведення негласних слідчих (розшукових) дій, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і документи або їх копії можуть використовуватися у доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування; 6) ст. 259 КПК України «Збереження інформації», у якій зазначено, що якщо прокурор має намір використати під час судового розгляду як доказ інформацію, отриману внаслідок втручання у приватне спілкування, або певний її фрагмент, він зобов'язаний забезпечити збереження всієї інформації. Враховуючи викладене, слід зазначити, що не менш важливим за отримання, в ході проведення НСРД, процесуально значимої інформації, є обізнане, своєчасне процесуальне оформлення отриманих результатів та закріплення їх як доказів.

Крім того, слідчому, прокурору необхідно пам'ятати, що категорії «матеріальний доказ» та «комп'ютерний (цифровий) доказ» тотожні лише з точки зору їх процесуального статусу і значення. Однак вони не тотожні з точки зору їх оформлення, зберігання та використання, тому що в цьому сенсі комп'ютерні докази оформлювати та використовувати набагато довше за часом і складніше за оформленням. Стосовно походження назви та поняття комп'ютерного доказу слушною є думка М. А. Іванова, який зазначав, що на початковому етапі мова йшла в основному про інформацію, яка створена за допомогою апаратних і програмних засобів комп'ютерної техніки, тому під час використання у кримінальному судочинстві як доказу така інформація отримала назву «комп'ютерний доказ» [9, с. 79]. Однак це визначення, на нашу думку, є дискусійним з огляду на теорію кримінального процесу.

Слід зазначити, що крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу про проведення НСРД, в ньому бажано фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення: 1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника; 2) серійний номер технічного засобу, пристрою, обчислювальної

техніки або програмного забезпечення; 3) наявний стан зношеності або будь-яких дефектів зовнішнього вигляду чи у роботі використаного технічного засобу, пристрою, обчислювальної техніки, програмного забезпечення (визначається зовнішнім візуальним оглядом слідчого чи оперативного працівника); 4) умови, у яких було використано технічний засіб, пристрій, обчислювальну техніку або програмне забезпечення, а також дату й точний час; 5) всю інформацію в цифровому вигляді, яка представляє процесуальний або оперативний інтерес незалежно від того, на якому носії вона знаходиться, бажано оглянути в присутності спеціаліста й понятих, після чого скопіювати її на матеріальний носій, який повинен бути долучений до протоколу проведення НСРД незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації [10, с. 303]; 6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диску комп'ютера, необхідно користуватись програмним забезпеченням для побітового копіювання інформації (наприклад, програми «SMART», «NED», «FTK»,«dd» тощо), а після копіювання до протоколу проведення НСРД необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено. Використання вказаних та інших вимог положень чинного КПК України слугуватиме більш ефективному застосуванню новітніх технологій у досудовому розслідуванні, зокрема під час проведення негласних слідчих (розшукових) дій, а також під час їх оформлення як слідчими, так і працівниками оперативних підрозділів, що виконують такі дії за їх дорученням. Однак окреслені питання потребують окремого дослідження або наукового вивчення.

Висновки. Розглянуті у статті питання є актуальними, своєчасними та такими, що підлягають подальшому дослідженню, оскільки узагальнення практики застосування негласних слідчих (розшукових) дій, їх організації та проведення, взаємодії між слідчим і працівником оперативного підрозділу не повне. Формування спеціалізованих регіональних оперативних підрозділів щодо протидії кіберзлочинності, які вийдуть з-під впливу керівників територіальних органів, висуває додаткове завдання щодо навчання такої категорії поліцейських, освоєння ними положень КПК України й у частині оформлення результатів НСРД у кримінальному провадженні, а також підвищення ними кваліфікації. Неузгодженості та неповнота положень чинного КПК України з цих питань, як свідчить наше дослідження, спонукають до їх доповнень, уточнень та удосконалення.

Список використаних джерел: **1.** Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – Київ : Юрінком Інтер, 2012. – 608 с. **2.** Зуйков Г. Г. Основные положения организации и методики расследования преступлений / Г. Г. Зуйков // Организация расследования преступлений : в 6 вып. : курс лекций. – М., 1991–1997. – Вып. 6. – 1977. – С. 15–18. **3.** Стецюк Б. Р. Етапи розвитку кримінального процесу в Україні (історико-правовий аспект) / Богдан Романович Стецюк // Впровадження нового Кримінального процесуального

кодексу України в правоохоронну діяльність та навчальний процес: досвід та шляхи удосконалення : матеріали наук.-практ. конф., м. Харків, 5 квіт. 2013 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків : Харків. нац. ун-т внутр. справ, 2013. – С. 61–64. **4.** Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / Д. М. Цехан ; за наук. ред. О. О. Подобного. – Одеса : Юрид. літ., 2011. – 214 с. **5.** Дубенко О. М. Збір та забезпечення доказів правопорушення, скоєного в Інтернеті / О. М. Дубенко // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : материалы Междунар. науч.-практ. конф. (Донецк, 8–19 мая 2006 г.). – Донецк : ДЮИ ЛГУВД, 2007. – С. 216–218. **6.** Колпакова О. В. Особливості розслідування злочинів у сфері комп'ютерної інформації / О. В. Колпакова // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : материалы Междунар. науч.-практ. конф. (Донецк, 8–19 мая 2006 г.). – Донецк : ДЮИ ЛГУВД, 2007. – С. 230–235. **7.** Голубев В. А. Противодействие киберпреступности и кибертерроризму / В. А. Голубев // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : материалы Междунар. науч.-практ. конф. (Донецк, 8–19 мая 2006 г.). – Донецк : ДЮИ ЛГУВД, 2007. – С. 29–42. **8.** Постіл Н. С. Класифікація слідів комп'ютерних злочинів / Н. С. Постіл, П. В. Цимбал // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : материалы Междунар. науч.-практ. конф. (Донецк, 8–19 мая 2006 г.). – Донецк : ДЮИ ЛГУВД, 2007. – С. 138–140. **9.** Иванов Н. А. Криминалистическое компьютероведение, компьютерная криминалистика и цифровые доказательства / Н. А. Иванов // Роль кафедры криминалистики юридического факультета МГУ им. М. В. Ломоносова в развитии криминалистической науки и практики : материалы Междунар. науч.-практ. конф. (Москва, 18–19 окт. 2010 г.) : в 2 т. / Моск. гос. ун-т им. М. В. Ломоносова. – М. : МАКС Пресс, 2010. – Т. 2. – С. 79–82. **10**. Доля Е. А. Формирование доказательств на основе результатов оперативно-розыскной деятельности : монография / Е. А. Доля. – М. : Проспект, 2009. – 357 с.

Надійшла до редколегії 28.03.2016

Юхно А. А. Особенности использования информационных технологий при проведении негласных следственных (розыскных) действий и их процессуальное оформление

Рассмотрены особенности использования современных информационных технологий при проведении негласных следственных (розыскных) действий, формы их процессуального оформления и закрепления в качестве доказательств в уголовном производстве. Описаны виды негласных следственных (розыскных) действий в соответствии с действующим УПК Украины и проанализированы возможности их применения в правоприменительной деятельности. Предложена авторская классификация современных информационных технологий. Проанализированы позиции учёных относительно поднятых в статье вопросов, дана авторская их оценка. Сделан вывод о наличии определённых несогласованностей и неполноты отдельных положений действующего УПК Украины.

Ключевые слова: досудебное расследование, уголовное производство, современные информационные технологии, негласные следственные (розыскные) действия, следователь, оперативный сотрудник, Интернет, современные технические средства и приспособления, вычислительная техника, программное обеспечение.

Yukhno O. O. Features of using information technologies in conducting secret investigative (search) actions and their procedural registration

The author has studied the features of modern information technologies in conducting secret investigative (search) actions, as well as forms of procedural registration and consolidation as evidence in criminal proceedings. Classification of secret investigative (search) actions under the current Criminal Procedural Code of Ukraine has been provided; possibilities of their use in law enforcement activities have been revealed. The author has carried out classification of modern information technologies by dividing them into the following two groups – concerning the use of modern technical equipment and devices and concerning the use of modern computers and software during secret investigation (search) actions.

Different points of view of scholars concerning the issues stated in the article have been analyzed. Peculiarities of assessment, tactical and procedural use and recording the results of secret investigative (search) actions during criminal proceedings and recognizing them as evidence have been separately analyzed. Special attention has been paid to the observance of such principles of criminal proceedings as the rule of law, legality, equality under the law and the court, guaranteeing the right to liberty and personal security, home or other property inviolability, secret of correspondence, non-interference in private life, spontaneity of evidence, objects and documents research, the presumption of innocence and providing proof of guilt, etc. It is emphasized that such actions are performed only on the basis of current legislation of Ukraine, including the criminal procedural one and the restriction of certain rights are carried out temporarily with the direct prosecutor and judicial control.

The author has concluded about the existence of certain inconsistencies and incompleteness of certain provisions of the current Criminal Procedural Code of Ukraine and the need for further study of these issues.

Keywords: pre-trial investigation, criminal proceedings, modern information technologies, secret investigative (search) actions, investigator, operative officer, Internet, modern technical equipment and devices, computers, software.