

УДК: 343.132

DOI: <https://doi.org/10.32366/2709-9261-2022-3-1-30-39>

Ковальова Ольга Вікторівна,
кандидат юридичних наук
(Донецький державний університет
внутрішніх справ, м. Маріуполь)
ORCID: <https://orcid.org/0000-0003-4555-0172>

ЗАСОБИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІД ЧАС ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ТА НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

У статті розглядаються особливості застосування засобів інформаційного забезпечення під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій. Звертається увага на те, що під правовими та організаційними засадами застосування засобів інформаційного забезпечення досудового розслідування необхідно розуміти вихідні положення, котрі регламентують особливості та нормативно встановлений порядок застосування засобів інформаційного забезпечення під час проведення досудового розслідування. Надається класифікація і характеристика сучасних засобів інформаційного забезпечення під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій.

Ключові слова: *засоби інформаційного забезпечення; слідчі дії; негласні слідчі дії; досудове розслідування; кримінальне процесуальне законодавство; кримінальне правопорушення.*

Постановка проблеми. Засоби інформаційного забезпечення, котрі застосовуються під час проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, у деякому сенсі є схожими з тими, що використовуються під час документування кримінальних правопорушень у межах оперативно-розшукової діяльності (особливо це стосується негласних слідчих (розшукових) дій). Це можна пояснити тим, що всі види діяльності в межах досудового розслідування спрямовані на реалізацію завдань, покладених на кримінальне процесуальне законодавство. При цьому варто звернути увагу на те, що процесуальний порядок та особливості застосування засобів інформаційного забезпечення під час проведення слідчих (розшукових) та негласних слідчих (розшукових) дій усе ж таки відрізняються, як і їхні види.

Аналіз останніх досліджень і публікацій. Питанням інформаційного забезпечення досудового розслідування приділялася увага багатьох українських учених. Різні аспекти були предметом аналізу вітчизняних науковців, зокрема І. В. Арістової, О. М. Бандурки, А. І. Берлача, А. М. Бірюкова, В. М. Брижко, В. Д. Гавловського, В. І. Галагана, В. О. Глушкова, І. О. Ієрусалімової, Р. А. Калюжного, Б. А. Кормича, О. В. Логінова, В. Г. Лукашевича, Є. Д. Лук'янчикова, А. М. Новицького, О. В. Олійника, Ю. В. Попова, В. М. Росоловського, О. С. Саїнчина та ін. Водночас чимало аспектів у межах зазначеної проблематики залишаються дискусійними.

Мета статті. Метою публікації є дослідження основних аспектів застосування засобів інформаційного забезпечення під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, а також аналіз перспектив використання останніх у сучасній українській науці та на практиці.

Виклад основного матеріалу. «Слідчі завдання, будучи односпрямованими, передбачають вибір різних способів та прийомів їх вирішення. Певне значення в процесі прийняття та реалізації слідчих рішень відіграє й інша інформація, яка міститься, зокрема, у такому джерелі, як автоматизовані інформаційні системи, наприклад в інформаційно-телекомунікаційній системі «Інформаційний портал Національної поліції України», яка, по суті, є інструментальним програмним засобом, що забезпечує інформаційно-аналітичну діяльність Національної поліції України, зокрема щодо формування баз (банків) даних, визначених ст. 26 Закону України «Про Національну поліцію» (далі – Закон), та надає доступ до інформації, котра формується та об'єднується в Єдиній інформаційній системі МВС України за певними ознаками» [1, с. 17–28]. Застосування вказаної інформаційно-телекомунікаційної системи під час здійснення слідчих дій дозволяє невідкладно отримати мінімальну інформацію, котра може бути інтегрована у процес досудового розслідування. Це зумовлено змістом цієї системи.

Так, у ст. 26 згаданого вище Закону України вказано, що: «1. Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно: 1) осіб, щодо яких поліцейські здійснюють профілактичну роботу; 2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду; 3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду; 4) розшуку осіб, зниклих безвісти; 5) установлення особи невідомих трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком; 6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій; 7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт); 8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією; 9) зареєстрованих кримінальних та адміністративних правопорушень, пов'язаних з корупцією, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах; 10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні; 11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян; 12) викрадених (втрачених) документів за зверненням громадян; 13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери; 14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків; 15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів

на рух окремих категорій транспортних засобів; 16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї; 17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася; 18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону. 2. Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК). 3. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством» [2]. Отже, у ресурсі наявна базова інформація, необхідна для закладення підґрунтя майбутнього доказового масиву.

У ст. 27 Закону зазначено: «1. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за умови обов'язкового дотримання Закону України «Про захист персональних даних». 2. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. 3. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України. В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів» [2]. У ст. 28 Закону вказано: «1. Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації. 2. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації. 3. Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 цього Закону» [2]. Отже, наведена норма призначена регулювати порядок та підстави застосування поліцією інформаційних масивів під час реалізації своїх завдань. Такий підхід обумовлений необхідністю захисту прав та свобод людини і громадянина, у тому числі – під час досудового розслідування.

«Інформаційний портал Національної поліції України складається з підсистем:

– «Гарпун», якою об'єднано інформацію про розшук транспортних засобів та номерних знаків, забезпечено оперативне реагування, моніторинг тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації на предмет їх розшуку, одночасного перебування на різних транспортних засобах (номерні знаки – двійники), використання номерних знаків, що, за даними Єдиного державного реєстру транспортних засобів МВС України, знищено, а також забезпечено взаємодію з державними та приватними

виконавцями під час розшуку транспортного засобу боржника у виконавчому провадженні;

– «Дорожньо-транспортна пригода», метою якої є автоматизація процесів оброблення органами (підрозділами) поліції інформації про дорожньо-транспортні пригоди (далі – ДТП), забезпечення проведення оцінювання стану аварійності тощо. Інформаційний ресурс цієї інформаційної підсистеми становить інформація, здобута в межах компетенції органами (підрозділами) поліції про ДТП, відповідно до кодів: про реєстрацію ДТП, характеристику місця ДТП (дорожні умови та дорожня обстановка), учасників, потерпілих, травмованих та загиблих, транспортні засоби та їх страхування;

– «Атріум», її метою є формування та наповнення електронного журналу контролю за прибуттям та взяття на облік раніше судимих осіб за встановленою формою, контролю за поведінкою осіб, щодо яких встановлено адміністративний нагляд, за прибуттям осіб, звільнених з місць позбавлення волі, до обраного ними місця проживання;

– «Слід», метою якої є: а) облік інформації про об'єкти, вилучені під час проведення слідчих (розшукових) дій, у єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного й телекомунікаційного обладнання; б) забезпечення інформаційно-аналітичного підтримання діяльності органів (підрозділів) поліції, спрямованого на запобігання кримінальним правопорушенням та їх розкриття; в) установлення зв'язків між даними, що мають значення для кримінального провадження; забезпечення оброблення інформації про об'єкти, вилучені під час проведення слідчих (розшукових) дій, наповнення та підтримання в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до системи «Інформаційний портал Національної поліції України».

У процесі прийняття та реалізації слідчих рішень має значення, крім уже згаданого вище джерела, й інша інформація, до якої належить:

– довідкова та консультативна інформація, отримана від співробітників експертно-криміналістичних та інших судово-експертних установ, осіб, які володіють спеціальними знаннями;

– інформація про трафік та контент, що міститься у відкритих базах даних та ресурсах (наприклад, телеграм-боти: @info_baza_bot; @HowToFind_RU_bot; @vkfindface_bot; Опендатабот; @getfb_bot; пошукові системи людей в інтернет-мережі за ім'ям, ніком, школою, адресою, електронною адресою, телефонним номером та іншими параметрами: peekyou.com; rip1.com; webmii.com; ussearch.com; spokeo.com; infobel.com; zabasearch.com; paginebianche.it; yasni.de)» [3, с. 293]. Таким чином, наведені інформаційні системи диференційовані за напрямками розслідуваної події та можуть бути використані залежно від особливостей кримінального правопорушення. Варто звернути увагу, що ці масиви мають значення не тільки у зв'язку з учиненням суспільно небезпечних діянь, а й для надання допомоги громадянам, пов'язаної із забезпеченням захисту їх прав і свобод. Так, наприклад, бази даних можуть бути застосовані для розшуку зниклих осіб, втрачених документів тощо. «Необхідну інформацію також можливо отримати в результаті пошуку на облікових записках у соціальних мережах: насамперед, слід зазначити, існують сайти, котрі здійснюють пошук імен та прізвищ відразу за всіма або декількома соціальними мережами, що істотно полегшує завдання пошуку: social-searcher.com – пошук

профілів у мережах за прізвищем, ім'ям у реальному часі; yandex.ru/people – пошук людей у мережах від Яндекс; uvrh.com – пошук Google за окремими соціальними мережами; poisksocial.ru – пошук у соціальних мережах. Звичайно, ці пошукачі за соціальними мережами не охоплюють абсолютно всі соціальні мережі, тому в окремих випадках більш раціонально здійснювати пошук напряму шляхом переходу на сайти соціальних мереж: Xing; Linked in; Twitter та ін.» [3, с. 293];

– інформація, що міститься в інтернет-мережі, окрім «видимої», включає також «невидиму» частину, ресурси якої можливо класифікувати на чотири типи: а) невидимість сторінок зумовлюється функціональними недоліками пошукових систем; б) сторінки умисно вилучені з індексації; в) сторінки, що потребують реєстрації, тобто згоди користувача щодо їх відвідування; г) власне «невидимий» сегмент мережі. Важливо звернути увагу на те, що, у разі необхідності збирання інформації в «невидимому» сегменті мережі потрібно використовувати спеціалізоване програмне забезпечення [3, с. 294];

– інформація, розповсюджена різними ЗМІ;

– інформація, отримана від представників громадськості, правозахисних організацій тощо;

– відомості, надані органами влади та управління [4, с. 360–370];

– інформація, отримана від осіб та організацій, які здійснюють приватну охоронну та детективну діяльність [3, с. 295].

Як і в процесі оперативно-розшукової діяльності, під час слідчих дій у ролі засобу інформаційного забезпечення може бути застосовано інтернет-мережу, зокрема особисті сторінки в соціальних мережах.

«У межах здійснення слідчих (розшукових) дій є і специфічні засоби інформаційного забезпечення, наприклад, пред'явлення особи для впізнання. Відповідно до чинного Кримінально-процесуального кодексу України (далі – КПК України) можна виділити пред'явлення особи для впізнання в натуральному вигляді та за його зображеннями (фотознімки, матеріали відеозапису). Пред'явлення особи для впізнання може проводитися за анатомічними (зовнішній вигляд і прикмети особи) та функціональними (голос, хода) ознаками (ч. 1, 9 ст. 228 КПК України). Оскільки у ст. 174 КПК України 1960 р. мова йшла тільки про зовнішній вигляд і прикмети особи, можливість пред'явлення її для впізнання за функціональними ознаками ставилася під сумнів, незважаючи на те, що на практиці проводилося. Впізнання може відбуватися в процесі безпосереднього контакту особи, що впізнає, з особами, яких пред'являють для впізнання, або поза візуальним та аудіоспостереженням з боку особи, яку пред'являють для впізнання. Впізнання за голосом у будь-якому випадку повинно здійснюватися поза візуальним контактом між особою, що впізнає, та особами, які пред'явлені для впізнання (ч. 9 ст. 228 КПК України). Пред'явлення для впізнання є видом криміналістичної ідентифікації за ідеальним відображенням (образом у думці) об'єкта (особи, речі тощо). Суб'єктом ідентифікації є людина, яка сприймала той чи інший об'єкт, запам'ятала його (зберегла у пам'яті його мислений образ) і може впізнати, якщо побачить знову. Саме мислений образ слід розглядати ідентифікуючим об'єктом, а не свідка, потерпілого, підозрюваного, як вважає В. О. Образцов» [5, с. 279]. Отже, у цьому контексті йдеться про застосування як засобу інформаційного забезпечення

ідентифікаційних особливостей людини, покладених в основу криміналістичної реєстрації.

«До наукового вивчення та прикладного дослідження проблеми використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій (далі – НСРД) 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, у 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 від 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» [6, с. 89]. Усі наведені технології входять до комплексу інформаційного забезпечення процесу досудового розслідування, котре відбувається шляхом накопичення та подальшого використання масиву даних. У науковій літературі вчені інколи зводять інформаційне забезпечення під час проведення негласних слідчих (розшукових) дій до використання вже наявної інформації, котра має обмежений доступ. Однак такий підхід є помилковим, оскільки зазначені дії, здебільшого, формують інформаційний комплекс, який застосовується для процесу доказування.

«Тому виникає необхідність підвищення якості знань працівників поліції у вказаних галузях та інформаційних технологіях. До першого напрямку 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 застосовувати наведені вище сучасні технічні засоби та пристрої, наприклад: 1) цифрові наддовгофокусні відеокамери, відеокамери з режимом зйомки в повній темряві, малі та надмалі пристрої прихованої аудіо-, відеофіксації доцільно використовувати під час проведення таких НСРД, як: а) аудіо-, відеоконтроль особи (ст. 260 КПК України); б) аудіо-, відеоконтроль місця (ст. 270 КПК України); 2) цифрові дзеркальні наддовгофокусні фото- та відеокамери, відеокамери з режимом зйомки в повній темряві, пристрої нічного бачення, малі та надмалі пристрої прихованої 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 КПК України); 3) відеокамери з режимом зйомки в 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 КПК України); 4) сучасні радіосканери доцільно використовувати під час проведення такої НСРД, як установа 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)» [6, с. 89]. Наведені технічні засоби призначені для фіксації та перевірки даних, які отримуються в ході здійснення негласних слідчих (розшукових) дій.

«Які конкретно технічні засоби необхідно використовувати в 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 указаних сучасних технічних досягнень і для запровадження у практичну діяльність. До другого напрямку 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 [7, с. 217], О. В. Колпакова [8, с. 233], В. О. Голубєв [9, с. 33], Н. С. Постіл і П. В. Цимбал [10, с. 138], слід класифікувати головні елементи аналітичної комп'ютерної розвідки, що доцільно застосовувати в 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. 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 систем». Така дія є найбільш доцільною та ефективною, ніж будь-яка інша НСРД» [6, с. 87]. «Під час проведення зазначених вище НСРД щодо цифрової інформації збір та аналіз кількісного і 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 перехоплювалася. Однак у такому випадку буде порушено негласність, а для вилучення і тимчасового доступу до комп'ютера будуть необхідні процесуальні підстави, тобто ухвала слідчого судді» [6, с. 87]. Отже, правові та організаційні засади застосування засобів інформаційного забезпечення досудового розслідування необхідно розуміти як вихідні положення, котрі регламентують особливості та нормативно встановлений порядок застосування засобів інформаційного забезпечення під час проведення досудового розслідування.

Висновки. Отже, розглянуті засоби інформаційного забезпечення можна поділити на: засоби техніко-програмного забезпечення – засоби, призначені для збору та фіксації даних у ході здійснення дій, передбачених кримінальним процесуальним законодавством, для отримання доказів у процесі досудового розслідування; засоби аналітико-комп'ютерного забезпечення – засоби, призначені для фактичного пошуку, документального оформлення та збереження матеріальної частини доказової бази; засоби інформативно-телекомунікаційного забезпечення – засоби, призначені для отримання доказів шляхом використання даних, котрі передаються на значні відстані за допомогою радіотехніки, комп'ютерної техніки та супутників; засоби інформативно-методичного забезпечення – інформаційні масиви, які використовуються як теоретичні знання з питань, що стосуються конкретної суспільно небезпечної події та її фігурантів.

Список використаних джерел

1. Дабіжа Д. В. Нормативно-правове забезпечення функціонування й розвитку автоматизованих інформаційних систем і їх підсистем, використовуваних органами (підрозділами) поліції. *Криміналістичний вісник*. 2020. № 2 (34). С. 17–28.
2. Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text> (дата звернення: 01.04.2022).
3. Бондар В. С. Інформаційні засади вирішення ситуаційних завдань під час досудового розслідування кримінальних правопорушень. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2021. № 2 (94). С. 278–299.
4. Лишак О. А., Круль С. М. Інформаційно-довідкові системи інших міністерств, відомств як складова інформаційно-довідкового забезпечення розслідування злочинів. *Криміналістика і судова експертиза*. 2019. Вип. 64. С. 360–370.
5. Образцов В. А. Криміналістика: курс лекцій. М., 1996. 448 с.
6. Юхно О. О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник Харківського національного університету*. 2016. № 2. С. 86–95.
7. Дубенко О. М. Збір та забезпечення доказів правопорушення, скоєного в Інтернеті. *Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения*: материалы Междунар. науч.-практ. конф. (г. Донецьк, 8–19 мая 2006 г.). Донецьк : ДЮИ ЛГУВД, 2007. С. 216–218.
8. Колпакова О. В. Особливості розслідування злочинів у сфері комп'ютерної інформації. *Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения*: материалы Междунар. науч.-практ. конф. (Донецьк, 8–19 мая 2006 г.). Донецьк : ДЮИ ЛГУВД, 2007. С. 230–235.
9. Голубев В. А. Противодействие киберпреступности и кибертерроризму. *Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения*: материалы Междунар. науч.-практ. конф. (г. Донецьк, 8–19 мая 2006 г.). Донецьк : ДЮИ ЛГУВД, 2007. С. 29–42.
10. Постіл Н. С., Цимбал П. В. Класифікація слідів комп'ютерних злочинів. *Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения*: материалы Междунар. науч.-практ. конф. (г. Донецьк, 8–19 мая 2006 г.). Донецьк : ДЮИ ЛГУВД, 2007. С. 138–140.

References

1. Dabizha, D. V. (2020). Normatyvno-pravove zabezpechennia funktsionuvannia y rozvytku avtomatyzovanykh informatsiinykh system i yikh pidsystem, vykorystovuvanykh orhanamy (pidrozdilamy) polit sii. *Kryminalistychnyi visnyk* [Regulatory and legal support for the functioning and development of automated information systems and their subsystems used by police bodies (units)]. *Forensic Bulletin*. № 2 (34). S. 17–28 [in Ukrainian].
2. Pro Natsionalnu polit siiu [About the National Police]: Zakon Ukrainy vid 2 lypnia 2015 roku № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text> (data zvernennia: 01.04.2022) [in Ukrainian].
3. Bondar, V. S. (2021). Informatsiini zasady vyrishennia sytuatsiinykh zavdan pid chas dosudovoho rozsliduvannia kryminalnykh pravoporushen. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka* [Information principles of solving situational tasks during the pre-trial investigation of criminal offenses. *Bulletin of Luhansk State University of Internal Affairs. E. O. Didorenko*]. № 2 (94). S. 278–299 [in Ukrainian].
4. Lyshak, O. A., Krul, S. M. (2019). Informatsiino-dovidkovi systemy inshykh ministerstv, vidomstv yak skladova informatsiino-dovidkovoho zabezpechennia rozsliduvannia zlochyniv. *Kryminalistyka i sudova ekspertyza* [Information and reference systems of other ministries, departments as a component of information and reference support of crime investigation. *Forensics and forensic science*]. Vyp. 64. S. 360–370 [in Ukrainian].
5. Obrazcov, V. A. (1996). *Kriminalistika: kurs lekcij* [Forensics: a course of lectures]. M. 448 s. [in Russian].
6. Iukhno, O. O. (2016). Osoblyvosti vykorystannia informatsiinykh tekhnolohii pid chas provedennia nehlasnykh slidchykh (rozshukovykh) dii ta yikh protsesualne oformlennia. *Visnyk Kharkivskoho natsionalnogo universytetu* [Features of the use of information technology during covert investigative (search) actions and their procedural design. *Bulletin of Kharkiv National University*]. № 2. S. 86–95 [in Ukrainian].
7. Dubenko, O. M. (2007). Zbir ta zabezpechennia dokaziv pravoporushennia, skoienoho v Interneti [Collection and provision of evidence of an offense committed on the Internet]. *Mezhdunarodne sotrudnychestvo v borbe s kompiuternoju prestupnostiu: problemy y puty ykh resheniya* : materyaly Mezhdunar. nauch.-prakt. konf. (Donetsk, 8–19 maia 2006 h.). Donetsk : DluY LHUVD. S. 216–218 [in Ukrainian].
8. Kolpakova, O. V. (2007). Osoblyvosti rozsliduvannia zlochyniv u sferi kompiuternoju informatsii [Features of the investigation of crimes in the field of computer information]. *Mezhdunarodne sotrudnychestvo v borbe s kompiuternoju prestupnostiu: problemy y puty ykh resheniya* : materyaly Mezhdunar. nauch.-prakt. konf. (Donetsk, 8–19 maia 2006 h.). Donetsk : DluY LHUVD. S. 230–235 [in Ukrainian].
9. Golubev, V. A. (2007). Protivodejstvie kiberprestupnosti i kiberterrorizmu [Countering cybercrime and cyberterrorism]. *Mezhdunarodne sotrudnychestvo v bor'be s komp'yuternoju prestupnost'yu: problemy i puti ih resheniya* : materyaly Mezhdunar. nauch.-prakt. konf. (Donetsk, 8–19 maia 2006 g.). Donetsk : DYUI LGUVD. S. 29–42 [in Russian].
10. Postil, N. S., Tsymbal, P. V. (2007). Klyasyfikatsiia slidiv kompiuternykh zlochyniv [Classification of traces of computer crimes]. *Mezhdunarodne sotrudnychestvo v borbe s kompiuternoju prestupnostiu: problemi y puty ykh resheniya* : materyaly Mezhdunar. nauch.-prakt. konf. (Donetsk, 8–19 maia 2006 g.). Donetsk : DluY LHUVD. S. 138–140 [in Ukrainian].

Kovalova Olha,

PhD in Law

(Donetsk State University of Internal Affairs, Mariupol)

ORCID: <https://orcid.org/0000-0003-4555-0172>

MEANS OF INFORMATION SUPPORT DURING INVESTIGATIVE ACTIONS AND SILENT INVESTIGATIVE ACTIONS

The article considers the means of information support during investigative actions and covert investigative actions. Attention is drawn to the fact that the legal and organizational basis for the use of information support of pre-trial investigation should be understood as the basic provisions governing the features and regulations of the use of information support during pre-trial investigation. The classification and characteristics of modern means of information support during investigative (investigative) actions and covert investigative (investigative) actions are provided. The issue of information provision of pre-trial investigation was paid to many Ukrainian scientists. At the

same time, many aspects within the specified issues remain debatable. The purpose of the publication is to study the main aspects of the use of information provisions during investigators (searched) actions and unclassified investigators (searched) actions, as well as an analysis of the prospects for the use of recent Ukrainian science and practice. Thus, the tools of information provision need to be divided into: means of food software - means for collecting and fixing data in the course of actions stipulated by the criminal procedural legislation for obtaining evidence in the process of pre-trial investigation; means of analytical and computer security - means intended for actual search, documentary design and preservation of the material part of the evidence base; means of informative and telecommunication support - means for obtaining evidence by using data that are transferred to significant distances for the help of radio engineering, computer equipment and satellites; Means of informative and methodological support - Information arrays are used as theoretical knowledge of issues relating to a particular socially dangerous event and its figures.

Key words: *means of information support; investigative actions; covert investigative actions; pre-trial investigation; criminal procedural legislation; criminal offense.*

Надіслано до редколегії 15.04.2022
Рекомендовано до публікації 22.04.2022