УДК 343.13:004
DOI https://doi.org/10.24144/2307-3322.2023.80.2.27

ДО ПИТАННЯ ВИКОРИСТАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСІ ЦИФРОВОЇ ІНФОРМАЦІЇ, ОТРИМАНОЇ ПІД ЧАС КОНТРРОЗВІДУВАЛЬНОЇ ТА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Метелев О.П.,
доктор філософії у галузі права,
завідувач спеціальної кафедри
Інституту підготовки юридичних кадрів
для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
ORCID: orcid.org/0000-0003-2969-8388

Коваленко Є.В.,
кандидат юридичних наук, професор спеціальної кафедри
Інституту підготовки юридичних кадрів
для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
ORCID: orcid.org/0000-0001-8630-8951

Метелев О.П., Коваленко Є.В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності.

У даній статті, спираючись на аналіз наукових публікацій та норм чинного законодавства, авторами досліджуються актуальні проблеми використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності. Аналізуються норми законодавства у сфері забезпечення державної безпеки та Кримінального процесуального кодексу України стосовно можливого використання цифрової інформації в якості доказів у судовому розгляді. Розглядаються наукові розробки та міжнародний досвід стосовно питань використання у цифровій формі матеріалів контррозвідувальної та оперативно-розшукової діяльності як доказів у кримінальному провадженні, в контексті їх допустимості. Авторами доводиться, що переважна більшість цифрової інформації, яка в подальшому може мати доказове значення, отримується шляхом проведення негласних заходів під час здійснення контррозвідувальної та оперативно-розшукової діяльності. Така цифрова інформація, на думку авторів, може слугувати лише приводами та підставами для початку досудового розслідування у кримінальному провадженні. У статті зазначається, що недостатня гармонізація кримінального процесуального законодавства та законодавства, що регулює контррозвідувальну і оперативно-розшукову діяльність, негативно впливає на ефективність виконання оперативними підрозділами своїх завдань. Також зазначається, що подальша реформа вітчизняної правоохоронної системи має рухатись за прикладом провідних західних країн та США, де поняття «оперативно-розшукова діяльність» взагалі відсутнє. У більшості зарубіжних демократичних країн світу таємне поліцейське розслідування є кримінально-процесуальною діяльністю, що являє собою гласні та негласні процесуальні дії, які здійснюються під керівництвом прокурора.

Автори статті роблять висновок, що для посилення контррозвідувальної складової у діяльності Служби безпеки України та враховуючи зарубіжний досвід у цій сфері, необхідно створити окремий, без посилання на вимоги положень Закону України «Про оперативно-розшукову діяльність» та Кримінальний процесуальний кодекс України, механізм організації та проведення заходів, пов`язаних із тимчасовим обмеженням прав і свобод людини.

Ключові слова: кримінальний процес, цифрова інформація, контррозвідувальна діяльність, оперативно-розшукова діяльність.

Metelev O.P., Kovalenko E.V. Regarding the issue of using digital information obtained during counterintelligence and investigative activities in criminal proceedings.

In this article, based on the analysis of scientific publications, the norms of the current legislation, the authors investigate the actual problems of using digital information obtained during counterintelligence and investigative activities in the criminal process. The norms of legislation in the field of ensuring state security and the Criminal Procedure Code of Ukraine regarding the possible use of digital information as evidence in court proceedings are analyzed. Scientific developments and international experience regarding the use of counterintelligence and investigative activity materials in digital form as evidence in criminal proceedings in the context of their admissibility are considered. The authors prove that the vast majority of digital information, which in the future may have evidentiary value, is obtained by conducting covert activities during the implementation of counterintelligence and investigative activities. Such digital information, according to the authors, can only serve as pretexts and grounds for starting a pre-trial investigation in criminal proceedings. The article notes that insufficient harmonization of criminal procedural legislation and legislation regulating counterintelligence and investigative activities negatively affects the effectiveness of operational units in performing their tasks. It is also noted that the further reform of the domestic law enforcement system should follow the example of leading Western countries and the USA, where the concept of "operational investigative activity" is absent at all. In most of the foreign democratic countries of the world, secret police investigation is a criminal procedural activity, which is overt and undercover procedural actions carried out under the direction of the prosecutor. The authors of the article conclude that in order to strengthen the counter-intelligence component in the activities of the Security Service of Ukraine and taking into account foreign experience in this area, it is necessary to create a separate, without reference to the requirements of the provisions of the Law of Ukraine "On Operational and Investigative Activities" and the Criminal Procedure Code of Ukraine, a mechanism for organizing and carrying out activities related to the temporary restriction of human rights and freedoms.

Key words: criminal process, digital information, counterintelligence activity, investigative activity.

Постановка проблеми. У сучасному інформаційному суспільстві постійно збільшується кількість людей, які використовують різноманітні цифрові технічні засоби, автоматизовані мережі і системи для створення, обробки та передачі інформації. Інформаційні технології засновані на використанні засобів електронно-обчислювальної техніки та електрозв'язку, одним із продуктів якої є цифрова інформація. На сьогодні такий вид інформації повністю охоплює всі сфери суспільних відносин, тому очевидно, що питання отримання цифрової інформації, яка може згодом набути статусу цифрових доказів, має важливе значення для ефективного забезпечення державної безпеки підрозділами Служби безпеки України (далі – СБУ). За своїм функціоналом, згідно положень ст. 24 Закону України «Про Службу безпеки України» співробітники СБУ здійснюють контррозвідувальну діяльність (далі – КРД), оперативно-розшукову діяльність (далі – ОРД) за кримінальними правопорушеннями, розслідування яких віднесено законодавством до компетенції СБУ, а також здійснюють досудове розслідування у кримінальних провадженнях [3]. Найбільш інформативним та надійним способом отримання достовірних цифрових відомостей під час здійснення КРД та ОРД є проведення негласних заходів, а під час досудового розслідування – негласних слідчих (розшукових) дій (далі – НСРД), оскільки ці заходи здійснюються в таємний спосіб, що знижує ймовірність навмисної модифікації чи знищення відомостей у цифровій формі, з огляду на їх швидкоплинність. Цифрова інформація, отримана за результатами проведення негласних заходів в рамках КРД та ОРД, міститься в файлах різних форматів представлення даних: фото-, відео-, аудіо-інформація, текстових документах, базах даних, електронних таблицях, службових лог-файлах, програмах і утилітах, які в подальшому можуть бути використані в доказуванні. Однак, використання матеріалів, отриманих в результаті здійснення КРД та ОРД, у кримінальному провадженні відповідно положень Кримінального процесуального кодексу України (далі – КПК) стикається у судовому засіданні з певними труднощами щодо визнання таких відомостей достовірними доказами, оскільки, по-перше такі фактичні дані отримані до внесення відповідної інформації до Єдиного реєстру досудових розслідувань (далі – ЄРДР), а по-друге, така цифрова інформація містить відомості, що становлять державну таємницю, розкриття яких у судовому засіданні може завдати суттєвої шкоди державній безпеці України. Розгляду та можливому вирішенню цих проблемних питань і присвячена ця стаття.

Стан дослідження. Не дивлячись на те, що відомості у цифровій формі, як результат проведення негласних заходів, складають значну частину доказової бази у кримінальному провадженні, питання використання цифрової інформації, отриманої під час здійснення КРД та ОРД, науковцями мало досліджене. На наш погляд, це пов'язано зі специфічною правовою природою цифрової інформації та необхідністю разом з процесуальними аспектами досліджувати деякі технічні аспекти роботи з цифровими відомостями. Водночас, окремі проблемні питання використання цифрової інформації та технологій у кримінальному провадженні, досліджували такі вітчизняні вчені як: Н.М. Ахтирська, М.В. Багрій, В.В. Білоус, М.В. Бондаренко, Н.В. Глинська, І.В. Гловюк, Д.І. Клепка, І.О. Крицька, В.В. Луцик, Ю.Ю. Орлов, Т.О. Павлова, Т.В. Михальчук, А.В. Скрипник, В.І. Сліпченко, О.С. Старенький, В.С. Стефанюк, А.В. Столітній, Д.М. Цехан, О.В. Шамрай та інші науковці. Також, проблемним питанням використання матеріалів КРД та ОРД у кримінальному процесі присвятили свої праці В.М. Бабакін, А.А. Венедіктов, О.В. Плетньов, М.А. Погорецький, Д.С. Сергєєва, А.О. Тимофєєв, С. Шульгін, М.Є. Шумило, М.В. Членов та інші процесуалісти.

Мета статті. Спираючись на аналіз наукових публікацій, норм вітчизняного законодавства та міжнародний довід, дослідити актуальні питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності і запропонувати можливі шляхи гармонізації законодавства у сфері забезпечення державної безпеки, а також кримінального процесуального судочинства.

Виклад основного матеріалу. Використання цифрової інформації для формування доказів у кримінальному процесі вже давно є сталою практикою, оскільки саме вона на сучасному етапі розвитку суспільства є найбільш розповсюдженим джерелом відомостей про людей та події. Цифрові доказові відомості є основними (але не єдиними) засобами ретроспективного пізнання учасниками кримінального провадження факту і обставин можливого кримінального правопорушення як минулої події соціальної реальності. Найбільш інформативними способами збирання доказових відомостей у цифровій формі є проведення окремих видів негласних слідчих (розшукових) дій (далі – НСРД) пов'язаних зі зняттям інформації з електронних комунікаційних мереж (ст. 263 КПК) та зняттям інформації з електронних інформаційних систем (ст. 264 КПК). Вибір даних способів збирання доказових відомостей органами досудового розслідування СБУ під час кримінального провадження щодо тяжких та особливо тяжких злочинів також обумовлений тенденцією збільшення кількості злочинів, які здійснюються з використанням засобів цифрової техніки, електронних комунікаційних мереж передачі даних, шкідливого програмного забезпечення та використання методів соціальної інженерії для отримання персональних ідентифікаційних даних осіб. Практика свідчить, що цифрові доказові відомості, отримані за результатами проведення НСРД, дозволяють одержати достовірні дані не тільки про осіб, причетних до вчиненого злочину, але й про можливих свідків протиправної події, потерпілих, про місця приховування знарядь злочину, предметів і документів, що містять інформацію про перебіг злочинних дій, невстановлені зв'язки підозрюваних осіб тощо. За допомогою цифрових слідів злочинів нерідко встановлюються особи, які зникли безвісти, місця переховування осіб, які знаходяться в розшуку, їх озброєність та інші дані, що можуть сприяти або, навпаки, перешкоджати їх затриманню. Матеріали, одержані в результаті проведення НСРД за ст. 263 та 264 КПК, дають можливість слідчому, або за його дорученням оперативному підрозділу, більш кваліфіковано проводити інші слідчі (розшукові) дії, ефективно реалізовувати оперативно-розшукову інформацію, створювати умови для проведення обшуку та інших слідчих дій» [6, с. 295].

Необхідно мати на увазі, що визначення допустимості і належності цифрових доказових відомостей для формування доказів, їх дослідження слідчим та подальша перевірка й оцінка в судовому засіданні мають певну специфіку обумовлену гносеологічною та правовою природою цифрової інформації, а саме:

– вони існують у нематеріальному вигляді;

– зберігаються на відповідному носії, в оперативній пам'яті електронно-обчислювальної машини або каналі зв'язку;

– для їх сприйняття та дослідження необхідні програмно-технічні засоби, тобто «посередники» між програмним кодом (цифровим сигналом) та людиною;

– вони мають здатність до дубляжу (копіювання/переміщення) на інший носій без втрати своїх характеристик;

– мають особливий статус оригіналу і можуть існувати у такому статусі у декількох місцях [8, с. 83]. Саме із цих причин до цифрових доказів пред'являються жорсткі вимоги, щодо належності, допустимості, правдоподібності для забезпечення їх надійності.

Як вже зазначалось, переважна більшість цифрових доказових відомостей отримуються в таємний спосіб шляхом проведення негласних заходів із застосуванням оперативно-технічних засобів. У кримінальному провадженні – це НСРД (Глава 21 КПК), під час здійснення ОРД використання оперативно-технічних засобів передбачено ст. 2 Закону України «Про ОРД», а під час здійснення КРД проведення оперативно-технічних заходів передбачено п. 1 ч. 2 ст. 7 Закону України «Про КРД» [1, 4, 5].

Слід зазначити, що СБУ, яка згідно ст. 5 Закону України «Про КРД» є спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності, здійснює контррозвідувальний пошук (в рамках КРД), а також під час ОРД, проводить оперативно-розшукові заходи з використанням оперативних та оперативно-технічних сил і засобів (п. 1 ч. 2 ст. 7 Закону України «Про контррозвідувальну діяльність») [4]. Крім того, відповідно до вимог ч. 2 ст. 214 КПК слідчі підрозділи СБУ, а за їх дорученням і оперативні підрозділи СБУ, можуть розпочати досудове розслідування після внесення відповідних відомостей про кримінальні правопорушення передбачені ч. 2 ст. 216 КПК (норма якої визначає підслідність здійснення досудового розслідування слідчими підрозділами СБУ) до ЄРДР [1].

З технічної точки зору, проведення негласних заходів в рамках здійснення КРД, ОРД та досудового розслідування мало чим відрізняються між собою, але кінцеві цілі проведення цих заходів різні. Ще раз підкреслюємо, що мета здійснення КРД кардинально відрізняється від мети здійснення ОРД та кримінального провадження. Так, відповідно до ст. 2 Закону України «Про контррозвідувальну діяльність» метою КРД є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення. Також, ст. 1 цього Закону визначено, що КРД – це спеціальний вид діяльності у сфері забезпечення державної безпеки. Також, п. 4 ч. 1 ст. 1 Закону України «Про національну безпеку» визначає державну безпеку як захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру [2].

В свою чергу, завданням здійснення ОРД є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави (ст. 1 Закону України «Про ОРД»).

Мета досудового розслідування витікає із загальної мети кримінального провадження. Погоджуємось з думкою Литвинчука О.І., який зазначив, метою досудового розслідування є забезпечення суду доказами та іншими необхідними матеріалами для здійснення правосуддя [7, ст. 220].

Тобто, ми бачимо, що здійснення КРД, на відміну від ОРД та досудового розслідування, апріорі не має на меті отримання будь-яких цифрових доказових відомостей, у тому сенсі, як вони розуміються у кримінальній процесуальній науці. В КРД мова йде про будь-яку інформацію (у тому числі цифрову), яка може допомогти органам та підрозділам СБУ забезпечити такий стан захищеності державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів який унеможливить, або суттєво знизить ймовірність реалізації реальних і потенційних загроз на шкоду державної безпеки України.

Звичайно, коли під час здійснення КРД (зокрема проведення оперативно-технічних заходів) підрозділами СБУ отримана відомості у цифровій формі про скоєний злочин, або злочин, що готується, то відповідно до ст. 214 КПК такі матеріали КРД можуть бути підставою, для здійснення досудового розслідування. Але використання матеріалів КРД у кримінальному процесі як можливих цифрових доказів, з нашої точки зору, доволі складно буде реалізувати. Основною проблемою тут може стати вимога ст. 23 КПК про безпосередність дослідження доказів у суді. Так, цифрова інформація, яка представляється суду для розгляду, міститься на цифровому носії інформації, який в свою чергу є додатком до протоколу проведення оперативно-технічного заходу. Для того щоб долучити цей цифровий носій з доказовими відомостями до справи та для того щоб згодом

він набув статусу судового доказу (за умов належності та допустимості), необхідно розсекретити протокол і цифровий носій – додаток до протоколу у повному обсязі. Тобто, неможливо виділити окремо матеріали, які містять цифрову інформацію про злочинну діяльність і інформацію, яка не підпадає під дію Кримінального кодексу України, але має суттєве значення для забезпечення державної безпеки в рамках здійснення КРД. Розкриття такої інформації в судовому засіданні зазвичай може нанести значної шкоди державним інтересам. Формат статті не дозволяє повністю розкрити всі аспекти такої діяльності, але практика показує, що цифрова інформація, отримана в результаті КРД може слугувати (не без виключень, звичайно) переважно лише підставами для початку проведення досудового розслідування та внесення відомостей до ЄРДР.

З використанням цифрової інформації, отриманої за результатами ОРД ситуація більш формалізована у законодавстві, хоча і тут, як зазначає М.Є. Шумило «особливої уваги заслуговує питання про взаємозв'язок оперативно-розшукових матеріалів і законності кримінально-процесуального провадження, оскільки відсутність правового механізму використання і перевірки достовірності оперативно-розшукових матеріалів при порушенні кримінальних справ нерідко стає причиною їх закриття» [10, с. 370]. Так, відповідно до ч. 2 ст. 99 КПК, матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про ОРД», за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази. На практиці, цифрові доказові відомості відносять або до речових доказів (наприклад, жорсткий диск або оперативна пам'ять, на яких може міститись доказово значима цифрова інформація) або до документів (матеріали цифрової фотозйомки, звукозапису, відеозапису та т. ін.). Оскільки у цифровій інформації, яка отримана шляхом проведення оперативно-технічних заходів, слідство переважно цікавить зміст, а не форма, то за відсутністю поки у КПК поняття «цифровий доказ», цілком логічно відносити таку доказово значущу цифрову інформацію до документів. А отже, використання таких матеріалів ОРД в кримінальному процесі припустимо.

Водночас, певні сумніви викликає питання використання цифрової інформації за результатами здійснення КРД та ОРД в якості можливих доказів у кримінальному провадженні в контексті їх допустимості. Згідно ст. 93 КПК «збирання доказів здійснюється сторонами кримінального провадження шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом». Під час кримінального провадження забезпечується принцип змагальності, у тому числі і через право сторони захисту ініціювати проведення НСРД, чого в рамках КРД та ОРД здійснити неможливо. Відтак вважаємо, що цифрова інформація, отримана під час здійснення КРД та ОРД може слугувати лише приводами та підставами для початку досудового розслідування.

До того ж, варто зазначити, що зараз для підрозділів СБУ загалом постає питання щодо доцільності здійснення ОРД. Так, на думку М.А. Погорецького прийняття у 2012 році нового КПК з одного боку вивело принцип змагальності у кримінальному процесі на кардинально новий рівень, а з іншого – поставило питання щодо доцільності такого виду державної діяльності як оперативно-розшукова діяльність. Науковець вважає, що цей термін існує з середини минулого століття та за своїм змістом включав у себе як розшукову роботу за фактом вчинення злочину, так і пошуково-розвідувальну роботу, спрямовану на попереджувальне виявлення осіб, що замишляють злочинну діяльність чи готуються до неї, причин та умов, що могли призвести до вчинення злочинів, а також їх окремі ознаки [9, С.58]. У КПК з 2012 року вже введене поняття НСРД, а слідчому надані повноваження проводити заходи (дії), що фактично є тотожними оперативно-розшуковим. Також, змінені підстави для проведення ОРД, яка тепер може проводитись тільки на стадії готування до вчинення злочину (п. 1 ч. 1 ст. 6 Закону «Про ОРД»). До того ж, більшість прав, що оперативні підрозділи мають згідно із Законом України «Про ОРД» (негласне обстеження публічно недоступних місць, житла чи іншого володіння особи, аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж, накладення арешту на кореспонденцію, здійснення її огляду та виїмки, установлення місцезнаходження радіоелектронного засобу, та інші) повинні реалізовуватись згідно із положеннями КПК. В свою чергу, бланкетною нормою є ст. 7 Закону

Україно «Про КРД», яка закріплює можливість вказаних заходів у порядку, передбаченому КПК України.

Практики ставлять справедливе, на наш погляд питання: «А для чого на цій стадії проводити ОРД, якщо можна за фактом готування до вчинення злочину внести данні до ЄРДР, відкрити кримінальне провадження та в рамках нього здійснити комплекс необхідних НСРД?». Теж саме стосується і КРД, під час здійснення якої процедура отримання санкції слідчого судді на проведення заходів, пов'язаних із тимчасовим обмеженням прав і свобод людини, займає досить тривалий час, що в умовах воєнного стану є невиправданим з точки зору своєчасності реагування на загрози національній безпеці.

Висновок. В умовах збройної агресії рф проти України, наша країна продовжує робити кроки у реформуванні державних інституцій та приведенні власного законодавства до європейських стандартів. Водночас, необхідно зазначити, що недостатня гармонізація законодавства, що регулює кримінальний процес, КРД та ОРД, негативно впливає на ефективність виконання оперативними підрозділами своїх завдань. Тому ми вважаємо, що подальша реформа правоохоронної системи має рухатись за прикладом провідних західних країн та США, де термін «оперативно-розшукова діяльність» не вживається. У більшості з них таємне поліцейське розслідування є кримінально-процесуальною діяльністю, що являє собою гласні та негласні процесуальні дії, котрі здійснюються поліцією під керівництвом прокурора (ФРН), або різними органами поліції (поліцейськими, детективами) та спеціально уповноваженими особами (Велика Британія, США та ін.) [9, С. 83].

В контексті посилення контррозвідувальної складової у діяльності СБУ, необхідно створити окремий, без посилання на вимоги положень Закону України «Про ОРД» та КПК, механізм організації та проведення заходів, пов`язаних із тимчасовим обмеженням прав і свобод людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 28.10.2023).
2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 22.10.2023).
3. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 25.10.2023).
4. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15 (дата звернення: 25.10.2023).
5. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 22.10.2023).
6. Кряковцев С.М. Дотримання особистих прав людини в процесі зняття інформації з транспортних телекомунікаційних мереж. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* Сєвєродонецьк, 2014. Вип. 2. С. 291–299.
7. Литвинчук О.І. Мета і завдання досудового розслідування. *Вісник Харківського національного університету імені В.Н. Каразіна № 1082. Серія «Право».* Випуск № 16, 2013. С. 219–221.
8. Метелев О.П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* Дніпро, 2018. № 1 (20). С. 75–86.
9. Погорецький М.А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: Монографія.-Х.: Арсіс, ЛТД. 2007, 576 с.
10. Шумило М.Є. Вибрані праці. Харків: Право, 2019. 1168 с.