УДК 343:98.322
DOI https://doi.org/10.32782/1813-338X-2023.4.37

Ю. С. Кононенко
аспірант кафедри кримінального процесу та криміналістики
Одеського державного університету внутрішніх справ

ТАКТИЧНІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПРИ РОЗСЛІДУВАННІ ДЕРЖАВНОЇ ЗРАДИ

Статтю присвячено дослідженню проведення окремих слідчих розшукових дій, як процесуального засобу отримання інформації щодо характеру злочинної події, способу виявлення, дослідження і збирання криміналістично значущої інформації при розслідуванні державної зради. Проведено оцінку сучасного стану правого регулювання та визначення особливостей проведення слідчих розшукових дій при розслідуванні державної зради, зокрема приділено увагу особливостям проведення огляду та обшуку.

Звертається увага, що основні напрями розслідування державної зради, конкретні методичні і тактичні рекомендації щодо проведення слідчих розшукових дій, залежать насамперед від форми вчинення держаної зради, змісту наявної інформації про подію та предмет злочину, способу його вчинення, правового статусу потенційного підозрюваного та іншої вихідної інформації, яка перебуває у розпорядженні слідчого як на момент внесення відомостей до ЄРДР, так і в подальшому. Характерною рисою розслідування державної зради, є те, що її форми вчиняються в умовах неочевидності, що в свою чергу вимагає активного проведення СРД, спрямованих на виявлення, збирання, фіксацію матеріальних джерел інформації одразу після початку досудового розслідування.

На підставі аналізу слідчої та судової практики встановлено, що по даній категорії кримінальних проваджень найчастіше проводиться огляд документів та комп'ютерних даних, зокрема інформації, яка міститься у відкритій мережі Інтернет, («Telegram»-каналах, акаунтах у соціальних сторінках осіб, причетних до злочину тощо). Огляд комп'ютерних даних є основним засобом збирання та дослідження електронних (цифрових) доказів під час досудового розслідування державної зради.

Визначено, що для забезпечення захисту, збереження інформації з відкритих джерел про факт державної зради та з метою безпосереднього її дослідження під час подальшого судового розгляду кримінального провадження, обов'язковою умовою фіксації має бути складання слідчим відповідного протоколу огляду, з урахуванням особливостей, передбачених Протоколом Берклі.

Ключові слова: *державна зрада, злочин, досудове розслідування, слідчі (розшукові) дії, тактичні особливості.*

Постановка проблеми. Ефективність досудового розслідування державної зради здебільшого залежить від успішного та своєчасного проведення слідчих розшукових дій (СРД), як процесуального засобу отримання інформації щодо характеру злочинної події, способу виявлення, дослідження і збирання криміналістично значущої інформації, яка з плином часу може бути втрачена. Зважаючи на це, для своєчасної реалізації завдань кримінального судочинства, тактику розслідування державної зради належить постійно забезпечувати новітніми засобами та методами проведення СРД, які спрямовані на збирання доказів у кримінальному провадженні. Таким чином, успіх роботи слідчого залежить від того, наскільки він тактично грамотно застосовує криміналістичні рекомендації з розслідування окремих видів злочинів і проведення окремих СРД [1, с. 28].

Аналіз останніх досліджень і публікацій. Окремі аспекти правового регулювання, а також тактичні та організаційні питання проведення окремих слідчих (розшукових) дій під час досудового розслідування в своїх роботах досліджували: Ю.П. Аленін, В.П. Бахін, В. С. Бондар, А.Ф. Волобуєв, Ю.М. Грошевий, В.А. Журавель, А.В. Іщенко, Н.І. Клименко, В.О. Коновалова, В.К. Лисиченко, О.Р. Михайленко, В.Т. Нор,

© Кононенко Ю. С., 2023

М.А. Погорецький, М.В. Салтевський, Р.Л. Степанюк, В.В. Тищенко, В.М. Шевчук, В.Ю. Шепітько, М.Є. Шумило, С. С. Чернявський, К.О. Чаплинський та інші. Проте розгляд тактичних особливостей проведення окремих слідчих (розшукових) дій при розслідуванні державної зради, не здійснювався.

Формування цілей. Метою статті є дослідження тактичних особливостей проведення окремих слідчих (розшукових) дій при розслідуванні державної зради.

Виклад основного матеріалу. Основні напрями розслідування державної зради, конкретні методичні і тактичні рекомендації щодо проведення СРД, а також тактичних операцій як на початковому, так і на наступних етапах розслідування залежать насамперед від форми вчинення держаної зради, змісту наявної інформації про подію та предмет злочину, способу вчинення злочину, правового статусу потенційного підозрюваного та іншої вихідної інформації, яка перебуває у розпорядженні слідчого як на момент внесення відомостей до ЄРДР, так і в подальшому. Характерною рисою розслідування державної зради, є те, що її форми вчиняються в умовах неочевидності, що в свою чергу вимагає активного проведення СРД, спрямованих на виявлення, збирання, фіксацію матеріальних джерел інформації одразу після початку досудового розслідування.

В цілому методика розслідування державної зради передбачає проведення на початковому етапі різноманітних СРД та інших процесуальних дій, специфікою з яких відрізняються насамперед огляд документів та комп'ютерних даних, які розміщені в електронних мережах (ст. 237 КПК України), допит свідків, потерпілих, підозрюваних (ст. ст. 225,224 КПК України); обшук житла чи іншого домоволодінні підозрюваних (ст. 234 КПК України), слідчий експеримент (ст. 240 КПК України), пред'явлення для впізнання (ст.ст. 228, 229 КК України), а також призначення та проведення судових експертиз (ст. ст. 242-245 КПК України).

Однак, застосування такого широкого комплексу процесуального інструментарію не завжди можливо у кримінальних провадженнях, які розпочаті за ознаками державної, особливо у формі переходу на бік ворога чи надання допомоги у проведенні підривної діяльності проти України, внаслідок вчинення таких злочинів на тимчасово окупованій території України, та перебування там більшості очевидців, свідків, документів, речових доказів та осіб, які підозрюються у вчинені таких злочинів. Аналіз слідчої та судової практики свідчить, що по даній категорії кримінальних проваджень найчастіше проводиться огляд документів та комп'ютерних даних, зокрема інформації, яка міститься у відкритій мережі Інтернет, («Telegram»-каналах, акаунтах у соціальних сторінках осіб, причетних до злочину тощо). Відповідно до статті 237 КПК України огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі) [2].

Досить поглиблені дослідження проблематики процесуальної організації і тактики проведення огляду комп'ютерних даних проведено А.В.Коваленко, який відзначає, що огляд комп'ютерних даних проводиться стороною обвинувачення з використанням електронно-обчислювальної техніки шляхом безпосереднього сприйняття аудіовізуального виразу комп'ютерних даних із метою отримання відомостей про факти, що мають значення для кримінального провадження. Такий огляд є основним засобом збирання та дослідження електронних (цифрових) доказів (електронних документів) під час досудового розслідування [3, с.55]. Слід погодитись із цілком справедливим твердженням А.В.Столітнього про те, що електронні докази – це інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84 КПК України, при цьому речові докази та документи будуть електронними доказами лише у випадку, коли їх джерелом є інформація, що зберігається (передається) в електронному вигляді [4, с. 148]. Під час розслідування державної зради електронні докази в мережі Інтернет можуть міститися на веб-сайтах, електронній пошті, соціальних мережах, у пошукових системах інформації тощо.

Слід відмітити, що у наукових дослідженнях останнім часом значна увага приділяється OSINT – розвідці з відкритих джерел. До переваг OSINT, на відміну від інших видів розвідки, відносять доступність джерел інформації, обсяг джерел інформації, різносторонність, оперативність отримання, легкість подальшого використання і вартість отримання [5, с. 127]. До інструментів та технологій OSINT, які можуть бути використані при розслідуванні державної

зради, відносяться: пошукові системи, соціальні мережі, офіційні та наукові сайти, онлайн карти, для збору інформації про підозрюваних осіб, їхню діяльність, освіту тощо. Зокрема, за допомогою пошукових систем (Google, Bing тощо) можна отримати інформацію про освіту, досвід роботи, належність до певних організацій, контактну інформацію підозрюваних осіб, тощо. Використання соціальних мереж (Facebook, Instagram, LinkedIn тощо) дозволяє здійснити аналіз особистих профілів підозрюваних та їх зв'язків з іншими особами або організаціями, зокрема надати інформацію про його діяльність та зв'язок з представниками держави-агресора, виявлення публікацій, які свідчать про проросійські погляди, тощо. Використання архівного сервісу: web.archive.org. дозволяє переглядати старі версії веб-сторінок, які могли бути змінені або видалені. Зокрема цей ресурс дає змогу проаналізувати архівні копії сторінок сайтів для вивчення інформації про підозрюваних осіб та їх діяльність. Геолокаційні інструменти: Google Maps, Google Earth дозволяють відстежити місця, пов'язані з підозрюваними, аналізувати їх маршрути, місця проживання та роботи. Зокрема Google Maps, може бути використано для перевірки адрес та розташування організацій, в якій працювали підозрювані тощо [6]. Отже, за допомогою інструментів та ресурсів OSINT можна отримати значну кількість доказів, які підтверджують участь підозрюваних осіб у протиправних діях. Зокрема: 1) зафіксувати та систематизувати доступні факти (дій, діяльності) підозрюваних осіб у ЗМІ, в тому числі в інтернет-ресурсах, на місцевому телебаченні тощо; 2) отримати аудіо-, фото- та відеосвідчення очевидців з числа місцевих жителів на окупованій території; 3) проаналізувати ЗМІ країни-терориста щодо висвітлення стану справ на окупованих територіях; 4) отримати оригінали/копії розпорядчих документів місцевих «керівників» населеного пункту, письмові заяви, відомості оплати праці та ін. [7, с.15].

Розглядаючи питання тактичних особливостей проведення огляду комп'ютерних даних, слід звернути увагу на застосування порядку виявлення та дослідження комп'ютерних даних, що зберігаються на носіях, запропонований О. В. Манжай: 1) аналіз доступних (відкритих) файлів шляхом контекстуального пошуку за ключовими фразами; 2) пошук прихованих і зашифрованих, тимчасових, специфічних даних; 3) спроба відновлення видалених файлів [8, с.112] У контексті досліджуваного питання слід погодитись з думкою А В.Коваленка, який указує на безпосередність візуального та аудіовізуального дослідження комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки. Адже комп'ютерні дані за своїм визначенням є інформацією, що була зашифрована для обробки логічними процесорами комп'ютерної техніки і, відповідно, в оригінальному вигляді не може бути сприйнята органами відчуття людини. Від так огляд комп'ютерних даних, як засіб збирання та дослідження доказів, з урахуванням вимог абз. 2 ч. 2 ст. 237 КПК України полягає в тому, щоб під час огляду цих даних уповноважені особи мали особисто сприйняти зміст аудіовізуального виразу комп'ютерних даних і відобразити його у протоколі СРД та додатках до нього у формі, придатній для сприйняття такого змісту іншими людьми [3, с.56].

Щодо фіксації комп'ютерних даних, то виходячи зі змісту ст. 104, абз. 2 ч. 2 ст. 237 КПК України, основною й обов'язковою формою фіксування є складання протоколу [2]. За загальним правилом, фіксація доказів в електронній формі, відбувається двома основні способи: 1) фіксація на аналоговому матеріальному носієві, властивості якого характеризуються безпосереднім і, як правило, відносно незмінним відображенням інформації (фото- та відеозапис); 2) фіксація на комп'ютерному носієві, фізичні властивості якого використовуються не для безпосереднього відображення інформації, а для записузчитування дискретних станів електромагнітного поля опосередковано через аналогово-цифровий перетворювач [9, с.25].

Відповідно до положень ч. 4 ст. 99 КПК України копія інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа [2]. Водночас суди, маючи на меті додержання засади безпосередності дослідження доказів, отриманих шляхом огляду інтернет-ресурсів, ставлять питання про дослідження в ході судового засідання інформаційного ресурсу, з якого виготовлена копія відповідної інформації, що не завжди може бути реалізовано через її видалення. Адже той спосіб фіксації, який зараз використовують, не забезпечує необхідного рівня перевірки, аудиту тих даних, які зберігаються і потім використову-

ються фактично як оригінал електронного документа чи цифрових даних [10].

З метою забезпечення допустимості та достовірності доказів з відкритих джерел рекомендовано застосовувати рекомендації щодо архівації даних, які містяться у відкритих джерелах. Слідчі, відповідні спеціалісти повинні чітко розуміти цей алгоритм дій, що надасть змогу захистити та зберегти інформацію з плином часу, включаючи забезпечення вимог щодо: справжності, доступності, ідентичності, постійності, рендерингу (візуалізації) та зрозумілості [11]. Адже належним чином зафіксовані та заархівовані дані є оригіналом цифрової інформації, яка, найчастіше, є визначальним, основним, а часом і єдиним доказом вини особи у вчиненні того чи іншого кримінального правопорушення. Саме на ці індикатори цифрової інформації, звертається увага у Протоколі Берклі, які підлягають захисту й збереженню [12].

Отже, для забезпечення захисту, збереження відповідної інформації з метою безпосереднього її дослідження під час подальшого судового розгляду кримінального провадження, обов'язковою умовою фіксації та збереження інформації з відкритих джерел про факт державної зради має бути складання слідчим відповідного протоколу огляду, з урахуванням особливостей, передбачених Протоколом Берклі – практичного посібнику з використання цифрової інформації з відкритим вихідним кодом [13]. Вважаємо, що використання Протоколу Берклі, при дослідженні цифрових відкритих джерел, є досить позитивною моделлю кримінального процесуального регулювання при розслідуванні державної зради. Безумовно, докази, отримані під час огляду Інтернет-ресурсів, мають бути перевірені та оцінені процесуальним шляхом.

Як демонструє слідча практика, при проведенні обшуку в ході розслідування аналізованого злочину, слід зосередити увагу на пошуку комп'ютерної техніки, комп'ютерних даних, електронних доказів. На підставі положень ст. 234 КПК України обшук проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, зокрема електронних доказів, відшукання знаряддя кримінального правопорушення, а також встановлення місцезнаходження розшукуваних осіб з обов'язковою участю не менше двох понятих незалежно від застосування технічних засобів фіксування відповідної слідчої (розшукової) дії [2]. Крім того, пошук та вилучення доказів в електронній формі можуть здійснюватися шляхом тимчасового вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, якщо вони безпосередньо зазначені в ухвалі суду відповідно до вимог ст. 168 КПК України [2] На відміну від огляду, при розслідуванні державної зради, обшук провадиться за наявністю достатніх підстав вважати, що публічне заперечення громадянином України здійснення збройної агресії проти України або публічні заклики громадянином України щодо підтримки рішень та/або дій держави-агресора та засоби, за допомогою яких вчинялася така діяльність, можуть мати значення для кримінального провадження та знаходяться певному приміщенні чи місці або в деякої особи. В результаті обшуку відбувається вилучення певних документів й предметів, що можуть мати значення письмових або речових доказів і знаходитися у володінні чи відданні конкретної особи або установи. Вилучення здійснюється тоді, коли слідчий має точні дані, що предмети чи документи, які мають значення для кримінального провадження, знаходяться у певної особи або певному місці. З метою найбільш ефективного пошуку слідів комп'ютерної інформації до провадження обшуку необхідно залучати спеціаліста з інформаційно-телекомунікаційних систем.

Під час обшуку, огляду чи тимчасового доступу до засобів комп'ютерної техніки створюють абсолютно ідентичний оригіналу екземпляр інформації у формі документа як процесуального джерела доказів. Слід наголосити, що власник, володілець або утримувач комп'ютерної системи, яку досліджують, можуть застосовувати різні способи захисту від копіювання. За такої умови ідентичне копіювання буде неможливим, що обґрунтовує фізичне вилучення носія електронної інформації під час обшуку або слідчого огляду для його вивчення та подолання систем захисту в процесі проведення відповідної судової експертизи [14, с.259].

Для підвищення ефективності проведення обшуку в приміщеннях, де знаходиться комп'ютерна техніка пропонуємо такий алгоритм: 1) збір інформації щодо кількості та типу засобів телекомунікацій та комп'ютерної техніки, виду електроживлення, підготовленності користувачів та технічного персоналу; 2) час проведення обшуку доцільно обрати на момент максимального робочого режиму та вжити захо-

дів до охорони комп'ютерної техніки; 3) залучення до участі та активна участь у проведенні обшуку спеціаліста (-ів) із використанням технічних та інших засобів [15, с.142]; 4) підбір понятих, бажано, проводити із числа осіб, які володіють знаннями у галузі комп'ютерної техніки; 5) вилучення попередньо зафіксованих файлових слідів-відображень та файлових слідів-предметів (залежно від обставин провадження) доцільно проводити шляхом: а) вилучення разом з носієм. У цьому випадку на попередньо виключеній комп'ютерній системі здійснюється від'єднання інтерфейсних та силових кабелів; б) вилучення окремо від носія: по-перше, шляхом вилучення даних, попередньо зафікосваних спеціалістом на власних носіях інформації (на переносні накопичувачі комп'ютерної інформації, та портативну комп'ютерну техніку) [16, с. 30][1]; по-друге, шляхом вилучення самих носіїв інформації (резервних копій даних комп'ютерної системи тощо). В даному випадку носії інформації вилучаються та залучаються до матеріалів кримінального провадження в якості речових доказів [15, с. 30].

Також, під час розслідування державної зради перед слідчими постає питання щодо витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей відповідно до п. 2 ст. 93 КПК України. Такими заходами можуть бути витребування відомостей від органів державної влади (військових частин, Департаменту з питань громадянства, паспортизації та реєстрації Державної міграційної служби, Державної прикордонної служби, управлінь МО України, державних установ виконання покарань, військово-цивільних адміністрацій, правоохоронних, судових та контролюючих органів) та місцевого самоврядування. Зокрема надані документи можуть стосуватись відомостей щодо: зафіксованості нанесення ракетно-авіаційних ударів та артилерійських обстрілів на певній території та пошкодження низки об'єктів; віднесення відомостей до інформації з обмеженим доступом відповідно до «Переліку відомостей Збройних сил України, що становлять службову інформацію (ПСІ-2017)», затвердженого наказом Генерального штабу Збройних Сил України від 22.11.2017 № 408, розголошення якої в умовах воєнного стану неуповноваженими на це особами створює загрозу для життя та здоров`я цивільних осіб і військовослужбовців, а також може бути використано державою, що здійснює збройну агресію проти України (інформація про розміщення військової техніки, зброї, озброєння, бойових припасів, а також дислокування за вказаними в переписці координатами підрозділів ЗСУ та інших військових формувань, які у відкритому доступі не розміщувалися); перебування конкретних осіб на території військових частини за визначений період з долученням документів та інших матеріалів, які підтверджують вищезазначену діяльність останніх (якими можуть бути копії з книг запису відвідувачів на КПП військової частини, копії з книг обліку порушень пропускного режиму військової частини; копії з книг обліку видачі одноразових перепусток військової частини тощо); правового статусу та місця знаходження військових частин; акти про проведення службових перевірок; проходження служби у відповідних військових частинах (витяги із наказів про зарахування на службу; витяги із наказів про звільнення в запас у зв`язку з позбавленням військового звання в дисциплінарному порядку); щодо перебування військовополонених у виправних колоніях, таборах для тримання військовополонених чи інших місцях позбавлення волі (характеристики; копії особової справи військовополоненого, в якій містяться документи, що посвідчують особу, в тому числі військовий квиток, виданий т. зв «лнр», «днр» та фотографії підозрюваних чи свідків); проходження ними військової служби в лавах окупаційних військ; картки-повідомлення про взяття в полон; довідками щодо перетину кордону (документи, що містять дані про конкретних осіб, в тому числі їх фотографії, що у сукупності можуть підтверджувати); перебування підозрюваного на обліку у психіатра чи нарколога; щодо перебування на відповідній посаді (копії наказів про призначення, переведення, звільнення, копію заяви про звільнення, характеристики); щодо реєстрації військової техніки та її військово-функціонального призначення, належності відповідній військовій частині; щодо розташування на певній місцевості дислокації ЗСУ, військової техніки, та її стану та готовності до виконання бойових завдань; щодо працівників, які виїхали з тимчасово окупованої території України, а також працівників, що залишились на цій території; інформації про розташування

[1] Одержання оперативно-розшукової інформації технічними засобами : монографія / [Л. І. Громовенко, Ю. Ф. Жаріков, І. П. Козаченко, Я. Ю. Кондратьєв, Ю. Ю. Орлов]. К. : НАВСУ, 2000. 364 с.

під час обстрілу лінії розмежування між ЗСУ й окупаційними організаціями тощо. Відповіді на ці запити нададуть реальну можливість встановити обставини вчинення державної зради у певній формі, зокрема визначити місце вчинення злочину, наслідки й інші відомості щодо події злочину як обставини, які підлягають доказуванню, відповідно до п. 1 ч. 1 ст. 91 КПК України. Подібна інформація може бути отримана також в порядку ст.ст 159-166 КПК України, якими регламентовано порядок тимчасового доступу до речей і документів.

Висновки. Підбиваючи підсумок, зазначимо, що тактичні особливості провадження слідчих (розшукових) дій на початковому етапі розслідування державної зради обумовлюються характером початкової слідчої ситуації, поведінкою підозрюваного, наявністю або відсутністю протидії розслідуванню з боку підозрюваного та інших зацікавлених осіб, стану наявної у слідчого інформації про обставини вчиненого злочину.

Список використаної літератури:

1. Іщенко А. В., Ієрусалимов І. О., Удовенко Ж. В. Теорія і практика криміналістичного забезпечення процесу доказування в розслідуванні злочинів : навч. посіб. Київ : Центр учб. літ., 2007. 224 с.
2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. Офіційний веб сайт. URL: https://zakon.rada.gov.ua/laws/show/4651-17
3. Коваленко А.В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий* вісник Херсонського державного університету. Серія *Юридичні науки*. 2023. Випуск 4. С.53-58. URL: https://lj.journal.kspu.edu/index.php/lj/article/view/393
4. Столітній А.В. Електронне кримінальне провадження на досудовому розслідуванні: дис. … докт. юрид. наук: 12.00.09 (081 – Право). Національна академія прокуратури України. Дніпропетровський державний університет внутрішніх справ, Дніпро, 2018. 648 с.
5. Шурат Т. Г., Смук А. О. Деякі аспекти розвідки з відкритих джерел інформації (OSINT). Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали всеукр. наук.-практ. конф. (м. Дніпро, 20 жовт. 2017 р.) : у 2-х ч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2017. Ч. 1. С. 126–128.
6. Блог Романа Радейка. Корисні фішки та цифрові інструменти для юристів. URL: https://onlinelawschool.pro/bloglaw/tpost/7f5nsu9yu1-yakosintnstrumenti-vikoristano-u-rozsldu
7. Вайда Т.С. Колабораційна діяльність в умовах війни: поняття, документування та кримінальна відповідальність за протиправні дії/діяльність. Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму : матеріали Всеукраїнської науково-практичної конференції (Одеса, 21 липня 2022 року). Одеса, 2022. С. 13–17.
8. Манжай О.В. Особливості огляду засобів комп'ютерної техніки. *Вісник* Харківського національного університету внутрішніх справ. 2016. № 3 (74). С. 111–120.
9. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 125 с.
10. Лист-орієнтування Офісу Генерального прокурора від 28.08.2021 № 18/1-386 вих. 515 окв 21 Керівникам обласних прокуратур «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел». https://zakononline.com.ua/documents/show/500229___686193
11. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. Портал Судової влади Укрїни. 07 червня 2022 р. URL:https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/
12. Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_ BerkeleyProtocol.pdf.
13. Проблеми доказування злочинів про колабораційну діяльність: аналіз прокурора Офісу Генерального прокурора. URL: https://www.helsinki.org.ua/articles/problemydokazuvannia-zlochyniv-pro-kolaboratsiynu-diialnist-analiz-prokurora-ofisu-heneralnohoprokurora/
14. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с. URL: https://doi.org/10.32837/11300.13264 с.259
15. Федотов О. А. Організація і тактика викриття приховування злочинів у сфері комп'ютерних технологій: дис…канд.. 12.00.09. Київ.2011. 239 с.
16. Одержання оперативно-розшукової інформації технічними засобами : монографія / [Л. І. Громовенко, Ю. Ф. Жаріков, І. П. Козаченко, Я. Ю. Кондратьєв, Ю. Ю. Орлов]. К. : НАВСУ, 2000. 364 с.

Kononenko Yu. S. Tactical features of conducting individual investigators (devocative) actions in the investigation of state treason

The article is devoted to the study of individual investigative search actions as a procedural means of obtaining information about the nature of the criminal event, the method of detection, research and collection of forensically significant information in the investigation of treason. An assessment of the current state of legal regulation and determination of the specifics of conducting investigative actions during the investigation of high treason was carried out, in particular, attention was paid to the specifics of the inspection and search.

Attention is drawn to the fact that the main directions of the investigation of high treason, specific methodological and tactical recommendations for conducting investigative investigative actions depend primarily on the form of committing high treason, the content of available information about the event and the subject of the crime, the method of its commission, the legal status of the potential suspect and other source information , which is at the disposal of the investigator both at the time of entering information into the EDPR and in the future. A characteristic feature of the investigation of state treason is that these forms are carried out in conditions of non-obviousness, which in turn requires active investigative actions aimed at identifying, collecting, recording material sources of information immediately after the start of the pre-trial investigation.

Based on the analysis of investigative and judicial practice, it was established that in this category of criminal proceedings, documents and computer data are most often reviewed, in particular, information contained in the open Internet, ("Telegram" channels, accounts on social pages of persons involved in crime, etc.). Computer data review is the primary means of collecting and examining electronic (digital) evidence during a pre-trial treason investigation.

It was determined that in order to ensure the protection, preservation of information from open sources about the fact of treason and for the purpose of its direct investigation during the further judicial review of the criminal proceedings, a mandatory condition of fixation should be the preparation of the appropriate inspection protocol by the investigator, taking into account the features provided for by the Berkeley Protocol .

Key words: *treason, crime, pre-trial investigation, investigative (search) actions, tactical features.*