УДК 343.1
DOI https://doi.org/10.24144/2788-6018.2026.02.3.28

ПРОБЛЕМНІ ПИТАННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Фещенко І.С.,
аспірант кафедри правового забезпечення безпеки бізнесу
Державного торговельно-економічного, адвокат
ORCID: 0009-0000-3527-1714

Фещенко І.С. Проблемні питання досудового розслідування кіберзлочинів.
У статті крізь призму думок вітчизняних науковців розглядається актуальна проблематика досудового розслідування кіберзлочинів в умовах стрімкої цифровізації суспільства та зростання ролі інформаційно-комунікаційних технологій у функціонуванні держави, економіки та критичної інфраструктури. Аналізується актуальний стан вітчизняної наукової розробки проблем досудового розслідування кіберзлочинів, теоретичних правових та практичних елементів здійснення досудового розслідування кіберзлочинів, здійснюється виокремлення в працях вчених найнагальніших проблем досудового розслідування кіберзлочинів. Доведено, що з огляду на стрімкий розвиток кіберзлочинності, виникнення все нових та більш сучасних способів та засобів вчинення кіберзлочинів має й стрімко розвиватися методика досудового розслідування таких злочинів. Встановлено, що різні аспекти процесу досудового розслідування кіберзлочинів привертають увагу багатьох вітчизняних вчених та науковців. Виявлено, що більшість вітчизняних науковців одностайні стосовно того, що здійснення досудового розслідування кіберзлочинів наразі вимагає як від слідчого, так й від інших представників правоохоронних органів спеціальних знань у цій сфері та широкого залучення до процесу досудового розслідування кіберзлочинів кваліфікованих експертів та спеціалістів. Встановлено, що приділення науковцями уваги до проблемних питань досудового розслідування кіберзлочинів сприяє виявленню проблемних питань в цьому процесі, пошуку шляхів їх подолання та вдосконалення досудового розслідування в цілому. Ідеї, які можуть бути запропоновані науковцями, можуть мати повністю новаторський характер стосовно проблем настання кримінальної відповідальності за злочини у сфері кібербезпеки в Україні. Встановлено, що окреслені вітчизняними науковцями актуальні проблеми досудового розслідування кіберзлочинів в Україні свідчать про необхідність комплексного підходу до їх вирішення. Доведено, що вдосконалення законодавства, модернізація технічного забезпечення, покращення кадрового потенціалу та розвиток міжнародної співпраці мають стати пріоритетними напрямами розвитку цієї галузі.
Ключові слова: кіберзлочин, кіберзлочинність, досудове розслідування, наукова проблематика.

Feshchenko I.S. The state of scientific development of problems of pre-trial investigation of cybercrimes.
The article examines the актуal problems of the pre-trial investigation of cybercrimes through the prism of the views of domestic scholars in the context of the rapid digitalization of society and the growing role of information and communication technologies in the functioning of the state, the economy, and critical infrastructure. The current state of national scientific research on the problems of pre-trial investigation of cybercrimes is analyzed, including the theoretical legal and practical elements of conducting such investigations, as well as the identification in scholarly works of the most urgent problems related to the pre-trial investigation of cybercrimes. It is proven that, given the rapid development of cybercrime and the emergence of increasingly modern methods and means of committing cybercrimes, the methodology of their pre-trial investigation must also develop rapidly. It is established that various aspects of the process of pre-trial investigation of cybercrimes attract the attention of many domestic scholars and researchers. It is revealed that most Ukrainian scholars agree that the pre-trial investigation of cybercrimes currently requires both investigators and other representatives of law enforcement agencies to possess specialized knowledge in this field and to widely involve qualified experts and specialists in the process of investigating cybercrimes. It is established that scholarly attention to the problematic issues of the pre-trial investigation of cybercrimes contributes to identifying the existing problems in this process, searching for ways to overcome them, and improving the pre-trial investigation as a whole. The ideas proposed by scholars may have a completely innovative character with regard to the problems of establishing criminal liability for cyber security offenses in Ukraine. It is also established that the актуal problems of the pre-trial investigation of cybercrimes in Ukraine identified by domestic scholars indicate the necessity of a comprehensive approach to their

resolution. It is proven that improving legislation, modernizing technical support, enhancing human resources potential, and developing international cooperation should become priority directions for the development of this field.

Key words: cybercrime, cybercrime, pre-trial investigation, scientific issues.

Постановка проблеми. Кіберзлочинність не стоїть на місці, тому не має відставати від нього й досудове розслідування кіберзлочинів. Відповідно досудове розслідування кіберзлочинів вимагає не тільки практичних навичок з боку службових осіб правоохоронних органів, але й теоретичних досліджень науковців, зосереджених на удосконаленні досудового розслідування кіберзлочинів, виявленні проблемних питань в цьому процесі й пошуків шляхів вирішення цих питань. Кількість та якість наукових досліджень особливостей та проблем застосування існуючих кримінально-правових процесуальних норм у зв'язку із вчиненням злочинів у сфері кібербезпеки в Україні відіграє важливу роль у процесі боротьби із злочинністю.

Мета дослідження – комплексний аналіз актуального стану наукової розробки проблем досудового розслідування кіберзлочинів, теоретичних правових та практичних елементів здійснення досудового розслідування кіберзлочинів, виокремлення в працях вчених найнагальніших проблем досудового розслідування кіберзлочинів.

Стан опрацювання проблематики. Огляд вітчизняних наукових праць за останні роки свідчить, що проблематика досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі активно досліджується вітчизняними вченими. Так, процес збирання, використання та застосування доказів кіберзлочинів досліджували І.О. Воронов, О.А. Самойленко, А.Ф. Волобуєв, Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан, М.О. Кравцова. У свою чергу, аналіз впровадження інноваційних засобів досудового розслідування кіберзлочинів є предметом уваги таких науковців, як В.А. Коршенко, В.М. Шевчук, А.С. Колодіна, Т.С. Федорова, І.М. Осика, А.О. Калюжна, О.А. Матвієнко та інших. Також питання, пов'язані з характеристикою, розслідуванням та протидією кіберзлочинності, у своїх працях досліджувало Н. М. Ахтирська, Л.Ю. Долженко, А.І. Марущак, Я.В. Неділько, О.С. Омельян, В.О. Точілов, В.Г. Хахановський та інші.

Виклад основного матеріалу. Сучасна соціально активна людина не може уявити своє життя без комп'ютерів, мобільних пристроїв, Інтернету за допомогою яких вона активно вступає у суспільні відносини в різних сферах суспільного життя. На шлях цифровізації та електронного документообігу переходить й держава й її органи, впроваджуючи надання державних послуг та ведення діловодства у цифровій формі.

Стабільна діяльність транспорту (зокрема залізничного, авіаційного), банківського сектору, фондових бірж, підприємств критичної інфраструктури й власне сама національна безпека держави безпосередньо залежить від стабільності та захищеності кіберпростору, в якому вони діють та який заснований на комунікації за допомогою електронних засобів зв'язку.

Однак, на жаль, завжди там, де виникає та розвивається новий вид суспільних відносин виникає та розвивається новий вид злочинності. В епоху високих технологій, тотальної цифровізації буквально усіх сфер людського буття та суспільних відносин, стрімкого розвитку цифрової реальності, хмарних технологій неможливо почувати себе повністю захищеним в кіберпросторі.

Сучасний швидкий розвиток цифрових технологій наприкінці XX століття – початку XXI століття спровокував таке нове явище у суспільстві як кіберзлочинність, якою є відповідна злочинна протиправна умисна діяльність як окремих фізичних осіб, так й цілих організованих злочинних груп й навіть державних структур, що здійснюється у цифровому середовищі (кіберпросторі) та/або за його допомогою з використанням стаціонарних та портативних комп'ютерів, мобільних пристроїв (планшетів, смартфонів), комп'ютерних мереж, мережі Інтернет, телекомунікаційних технологій (бездротові Wi-Fi, Bluetooth, WiMAX тощо), поширення шкідливих комп'ютерних програм, взлому баз даних, рахунків, особистих аккаунтів тощо.

Згідно положень пункту 8 частини першої статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII (із змінами) кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У свою чергу, кіберзлочинність є сукупністю кіберзлочинів (пункт 9 частини першої статті 1 Закону України «Про основні засади забезпечення кібербезпеки України») [1].

Досудове розслідування згідно положень пункту 5 частини першої статті 3 Кримінального процесуального кодексу України від 13 квітня 2012 року № 4651-VI (із змінами) – це стадія кримінального провадження, яка починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується закриттям кримінального прова-

дження або направленням до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності, клопотання про закриття кримінального провадження [2].

Відповідно, з огляду на особливості кіберзлочинності, способи та засоби вчинення кіберзлочинів на сьогодні проблематика досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі доволі активно досліджується у наукових працях (наукових статтях та цілих наукових монографіях) вітчизняних вчених.

Так, до основних ознак кіберзлочинності Харитоненко І.О. відносить наступні: кіберзлочини є неперсоніфікованими та анонімними, вони вчиняються у кіберпросторі, віддаленість кіберзлочинів, тобто жертву та кіберзлочинця можуть розділяти тисячі кілометрів, кіберзлочинність характеризується високим рівнем латентності, наявність відповідного рівня знань та навиків у даній сфері [3, с. 402].

Самойленко О.А. зазначає, що унаслідок вчинення злочинів у кіберпросторі утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких справах широкого спектру судових експертиз, а саме: експертизи комп'ютерної техніки і програмних продуктів, експертизи телекомунікаційних систем (обладнання) та засобів, технічної експертизи документів, експертизи відеозвукозапису, експертизи у сфері інтелектуальної власності, інших видів експертиз, без проведення яких неможливо отримати необхідні відомості, що свідчать про ознаки складу одного зі злочинів злочинної сукупності (наприклад, економічних експертиз, психологічної, мистецтвознавчої експертизи або відповідної комплексної експертизи; трасологічних експертиз, лінгвістичної експертизи мовлення (семантикотекстуальний аналіз писемного й усного мовлення), судово-балістичних, судово-хімічних експертиз тощо [4, с. 298-299].

Досліджуючи проблему розслідування кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, Вейц А.М. наголошує на трьох її складових: 1) створення підроблених (фіктивних) Інтернет-сторінок державних органів, підприємств, електронних платіжних систем, відомих фірм та компаній. В планах розслідування таких злочинів основна версія щодо способу їх вчинення пов'язана із шахрайським обманом шляхом вчинення фіктивного представництва. Для слідчого в такому випадку винний не співвідноситься з установою-жертвою, створюється враження про свою неналежність до того чи іншого державного підприємства або установи, банка тощо. За такої обставини розслідування повинно тривати до моменту встановлення складу всіх учасників групи, що надасть можливість попередити наступний епізод злочинної діяльності із участю спеціального суб'єкту; 2) у криміналістичному аспекті злочинна діяльність у кіберпросторі являє собою систему об'єднаних загальними мотивами і цілями злочинних дій, операцій та епізодів, розраховану на відносно тривалий період і підготовку, що включає в себе планування, здійснення, маскування та протидію її викриттю. З цією метою злочинці вдало застосовують технології анонімізації доступу до ресурсів електронних інформаційних мереж, зокрема мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій, або Virtual Private Network) інших засобів-анонімайзерів); 3) тиск на слідчого чи прокурора з боку корумпованих представників влади підчас розслідування кіберзлочинів [5, с. 392-393].

Вейц А.М. також підкреслює, що в сучасних реаліях перед правоохоронними органами, залученими до проведення досудових розслідувань кіберзлочинів, вчинених у військовому середовищі постає низка проблемних питань, таких як: 1. фіксація обстановки вчинення кіберзлочину та слідової картини, 2. існування ризику для особистої безпеки слідчого, представників правоохоронних органів під час проведення слідчих (розшукових) дій на території ведення активних бойових дій, 3. наявність спеціального суб'єкта кримінального правопорушення, 4. можлива протидія з боку командирів військових підрозділів у випадках неналежного виконання ними службових обов'язків, що стало умовою вчинення кримінального правопорушення їх підлеглим [6, с. 240].

Відтак, на думку науковця, наявна потреба в розробці нових підходів до розслідування кіберзлочинів, які враховують специфіку військового середовища, технологічні інновації та досвід бойових дій на території України [6, с. 234].

Кононенко М.П. досліджуючи питання сучасного процесуального керівництва досудовим розслідуванням кримінальних правопорушень, вчинених у кіберпросторі або з його використанням дійшов висновку, що варто реалізувати новий підхід до того, як виявляти і розслідувати кіберзлочини, адже заходи й методи, якими користуються, щоб документувати традиційні злочини, в цій галузі – нерезультативні. На думку науковця, в царині, де діють високі технології, необхідно, аби наукові, технічні та інші спеціальні знання мали не тільки фахівці, а й слідчі органи внутрішніх справ, прокурори, слідчі та судді. Тож, особливо слід зосередитися на тому, аби вдосконалювати професійну підготовку праців-ників органів досудового розслідування та прокурора. Оскільки у

зв'язку з її недостатнім рівнем можуть бути допущені й допускаються помилки, коли застосовуються кримінально-процесуальні та кримінально-правові норми [7].

Аналогічних висновків, що використання спеціальних знань шляхом залучення спеціаліста чи експерта значно підвищить результативність та полегшить роботу слідчого під час досудового розслідування кіберзлочинів дійшла у своїх дослідженнях й Линник О.В. [8, с. 118].

Проблемні питання розслідування кіберзлочинів, пов'язаних із втручанням у роботу банкоматів досліджував Криволапов В.М. Вчений наголосив, що специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців [9, с. 139-140].

На думку Дунаєвої Т.Є., яка досліджувала особливості предмету доказування кіберзлочинів в Україні під час воєнного стану проблема полягає в тому, що в умовах цифровізації життя, доцільно і удосконалити збір та збереження доказів, що стосуються кіберзлочинності. Тому постає питання про підвищення якості кримінального процесуального законодавства України шляхом внесення відповідних змін до КПК України у частині підвищення ефективності доказування кіберзлочинів [10, с. 56].

На думку Коцмана І.І. відсутність єдиного підходу до розуміння поняття «кіберзлочинність» тягне за собою такі проблеми, як розбіжності у державному регулюванні кіберзлочинності. Вчений наголошує, що саме тому необхідною є гармонізація міжнародного та національного законодавства у сфері кіберзлочинності, внесенням відповідних змін у кримінальне та кримінальне процесуальне законодавство України, оскільки під час досудового розслідування кіберзлочинів і судового розгляду справ виникають проблеми, зокрема, при оцінці судом електронних доказів [11, с. 245, 250].

Досліджуючи проблематику досудового розслідування кіберзлочинів, а також причин, що їх обумовили, недоліки збирання доказової інформації при розслідуванні кіберзлочинів, зокрема тих, що пов'язані з призначенням судових експертиз, науковець Омелян О.С. відмітив найбільш актуальну проблему, що виникає під час розслідування кіберзлочинів: неякісне збирання доказів під час оглядів та обшуків. Наприклад, обладнання комп'ютерних систем (це може бути автоматизована система, яка піддавалася кібератаці, або комп'ютер чи система з кількох комп'ютерів та телекомунікаційне обладнання зловмисника тощо) вилучається без належної фіксації її у зібраному стані. В результаті у майбутньому стає неможливим проведення слідчого експерименту або проведення судової експертизи, оскільки неможливо з'єднати складові, як вони були поєднані у початковому стані [12, с. 412].

На важливості залучення експертів та спеціалістів на стадії досудового розслідування кіберзлочинів з метою отримання консультацій, а в подальшому проведення експертиз та складання висновків наголошують також Г.В. Муляр та О.С. Ховпун [13, с. 137].

На необхідність залучення осіб, що володіють спеціальними знаннями до проведення слідчих дій при досудовому розслідуванні кіберзлочинів звертають увагу й Є.Д. Лук'янчиков та Б.Є. Лук'янчиков, підкреслюючи, що використання допомоги зазначених осіб дозволить своєчасно визначати індивідуальний почерк роботи програміста й ідентифікаційних характеристик розроблених ним програм, перелік електронних адрес і сайтів Інтернет, якими оперував користувач. Спеціаліст допоможе дослідити матеріальні носії з метою пошуку відповідної інформації та провести ідентифікацію комп'ютерних систем за слідами на різних матеріальних носіях інформації [14, с. 114].

Розумний С. в ході проведеного ним ґрунтовного аналізу думок науковців та правоохоронної практики розслідування кіберзлочинів дійшов висновків, що використання спеціальних знань під час розслідування кіберзлочинів сприяє отриманню об'єктивної та повної доказової інформації, розширює можливості слідчого в отриманні доказів [15, с. 210].

Висновки. Підсумовуючи можна зазначити, що з огляду на стрімкий розвиток кіберзлочинності, виникнення все нових та більш сучасних способів та засобів вчинення кіберзлочинів має й стрімко розвиватися методика досудового розслідування таких злочинів. Необхідно відмітити, що різні аспекти процесу досудового розслідування кіберзлочинів привертають увагу багатьох вчених та науковців. Більшість науковців одностайні стосовно того, що здійснення досудового розслідування кіберзлочинів наразі вимагає як від слідчого, так й від інших представників правоохоронних органів спеціальних знань у цій сфері та широкого залучення до процесу досудового розслідування кіберзлочинів кваліфікованих експертів та спеціалістів, оскільки відсутність спеціальних знань в цій сфері значно ускладнює успішне розслідування вчинених кіберзлочинів. Про конкретні практичні

проблеми досудового розслідування кіберзлочинів можуть знати лише працівники органів досудового розслідування, які безпосередньо з ними стикаються в процесі своєї службової діяльності, проте які, на жаль, не часто можуть виносити їх у загальну наукову площину для пошуків науковцями шляхів їх вирішення. Відповідно, й наукова розробка проблем досудового розслідування кіберзлочинів може ґрунтуватися на аналізі науковцями положень нормативно-правових актів в цій сфері та наявної судової практики, доступ до якої є відкритим для громадськості. Окреслені науковцями актуальні проблеми досудового розслідування кіберзлочинів в Україні свідчать про необхідність комплексного підходу до їх вирішення. Вдосконалення законодавства, модернізація технічного забезпечення, покращення кадрового потенціалу та розвиток міжнародної співпраці мають стати пріоритетними напрямами розвитку цієї галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон від 05.10.2017 № 2163-VIII. База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 01.03.2026).
2. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 № 4651-VI. База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення 01.03.2026).
3. Харитоненко, І. (2020). Феномен кіберзлочинності в сучасній кримінологічній теорії. *Часопис Київського університету права*, (4), 401-404. https://doi.org/10.36695/2219-5521.4.2020.72 (дата звернення: 01.03.2026).
4. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст]: монографія / О.А. Самойленко; за заг. ред. А.Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с. https://doi.org/10.32837/11300.13264 (дата звернення: 01.03.2026).
5. Вейц А.М. Проблеми розслідування кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг. Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України): у 2 т.: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С.В. Ківалова. Одеса: Видавничий дім «Гельветика», 2021. Т. 2. С. 391-394. URL: https://hdl.handle.net/11300/15499 (дата звернення: 01.03.2026).
6. Вейц А.М. Особливості розслідування кіберзлочинів, вчинених у військовому середовищі. *Інформація і право*. 2024. № 4. С. 233-242. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001573645 (дата звернення: 01.03.2026).
7. Кононенко М.П. (2024). Процесуальне керівництво досудовим розслідуванням кримінальних правопорушень, вчинених у кіберпросторі або з його використанням. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*, (12). https://doi.org/10.54929/2786-5746-2024-12-01-14 (дата звернення: 01.03.2026).
8. Линник О.В. Використання спеціальних знань під час розслідування кіберзлочинів. Сучасні тенденції розвитку криміналістики та кримінального процесу. Тези доповідей міжнародної науково-практичної конференції до 100-річчя від дня народження професора М.В. Салтевського (м. Харків, 8 листопада 2017 р.). Харків. 2017. С. 116-118. URL: https://univd.edu.ua/general/publishing/konf/08_11_2017/pdf/51.pdf (дата звернення: 01.03.2026).
9. Криволапов В.М. Проблемні питання розслідування кіберзлочинів, пов'язаних із втручанням у роботу банкоматів. Актуальні проблеми досудового розслідування. Міжвідомча науково-практична конференція (Київ, 5 липня 2017 року). С. 137-140. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/4abe7c4c-8b4f-4875-98be-8ee0fade2dd8/content (дата звернення: 01.03.2026).
10. Дунаєва Т.Є. Особливості предмету доказування кіберзлочинів в Україні під час воєнного стану. *Dictum factum*. - 2022. № 2. С. 55-59. URL: https://df.duit.in.ua/index.php/dictum/article/view/231 (дата звернення: 01.03.2026).
11. Коцман І.І. Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки. *Public management and administration in Ukraine*. 2024. № 40. С. 245–252. https://doi.org/10.32782/pma2663- 5240-2024.40.41 (дата звернення: 01.03.2026).
12. Омелян О.С. Актуальні проблеми досудового розслідування кіберзлочинів. Актуальні питання судової експертології, криміналістики та кримінального процесу: мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.) / за заг. ред. О.Г Рувіна, Н.В. Нестор; уклад. О.І. Жеребко, А.О. Полтавський, О.В. Юдіна. К.: КНДІСЕ Мінюста України, 2019. 672 с. С. 410-414. URL: http://revopravo.kiev.ua (дата звернення: 01.03.2026).

13. Муляр Г.В. Особливості доказування кіберзлочинів . *Право. Людина. Довкілля*. 2019. Vol. 10, № 3. С. 132-138. URL: http://nbuv.gov.ua/UJRN/lHE_2019_10_3_19 (дата звернення: 01.03.2026).
14. Лук'янчиков Є.Д. Участь спеціаліста в розслідуванні комп'ютерних злочинів. Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практич. конф.: м. Харків, 10 груд. 2013 р. / МВС України, Харків. нац. ун-т внутріш. справ. Київ: ВАІТЕ, 2013. С. 113-115. Бібліогр.: с. 115. URL: https://library.nlu.edu.ua/POLN_TEXT/SBORNIKI_2018/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf (дата звернення: 01.03.2026).
15. Розумний С. Використання спеціальних знань при розслідуванні кіберзлочинів. *Науковий вісник Дніпровського державного університету внутрішніх справ*. № 1/2023. Спеціальний випуск. С. 205-212. http:// doi.org / 10.31733/2078-3566-2023-5-205-212 (дата звернення: 01.03.2026).

Дата першого надходження рукопису до видання: 1.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026