До разової Спеціалізованої вченої
ради Національного університету
«Одеська юридична академія»

РЕЦЕНЗІЯ

рецензента, доктора юридичних наук, професора
Торбаса Олександра Олександровича
на дисертацію **Філімонова Микити Володимировича**
на тему: **«Особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі»,**
подану на здобуття ступеня доктора філософії за спеціальністю 081 – «Право»

Актуальність теми дисертаційного дослідження. Сучасний етап розвитку інформаційного суспільства характеризується стрімким поширенням цифрових технологій, інтернет-комунікацій та інформаційних систем, що зумовлює трансформацію традиційних форм суспільних відносин. Разом із позитивними наслідками цифровізації зростає і рівень кримінальних правопорушень, що вчиняються із використанням інформаційно-комунікаційних технологій або безпосередньо в кіберпросторі. Такі правопорушення відзначаються високим рівнем латентності, транскордонним характером, складністю ідентифікації суб'єктів та специфічністю слідів кримінально протиправної діяльності. У зв'язку з цим особливого значення набувають питання ефективного здійснення досудового розслідування таких кримінальних правопорушень, центральним елементом якого є процес доказування.

Актуальність дослідження зумовлена тим, що доказування у кримінальних провадженнях щодо правопорушень, вчинених у кіберпросторі, характеризується низкою специфічних особливостей, пов'язаних із використанням електронних доказів, необхідністю використання спеціальних знань у сфері інформаційних технологій тощо. Наявні процесуальні механізми не завжди повною мірою відповідають сучасним викликам, що виникають у сфері кіберзлочинності, а практика їх застосування свідчить про існування значної кількості проблем у збиранні, перевірці та оцінці доказів. У цих умовах наукове осмислення особливостей доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, має важливе теоретичне та практичне значення для підвищення ефективності кримінального провадження.

Наукова обґрунтованість представлених теоретичних та/або експериментальних результатів проведених здобувачем досліджень. Метою дисертаційного дослідження є вирішення наукового завдання, яке полягає у формулюванні цілісної концепції кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Для досягнення поставленої мети у дисертації вирішувались такі завдання: 1) з'ясувати стан наукового дослідження проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі; 2) уточнити поняття кіберпростору та кримінальних правопорушень, вчинених у кіберпросторі; 3) виокремити основні стандарти, які сформовані у практиці ЄСПЛ щодо забезпечення права на повагу до приватного життя у кіберпросторі; 4) виокремити міжнародні стандарти та узагальнити зарубіжний досвід розслідування кримінальних правопорушень, вчинених у кіберпросторі; 5) уточнити поняття електронних (цифрових) доказів у кримінальному провадженні та здійснити їх класифікацію; 6) встановити поняття та зміст джерел електронних (цифрових) доказів у кримінальному провадженні; 7) з'ясувати особливості проведення слідчих (розшукових) дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі; 8) з'ясувати особливості проведення негласних слідчих (розшукових) та інших процесуальних дій при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі;

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим у вітчизняній науці кримінального процесу комплексним дослідження теоретичних та практичних проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі на основі положень КПК України 2012 року.

У межах проведеного наукового дослідження одержано такі результати, що мають наукову новизну:

вперше:

– визначено коло даних, які можуть міститися у хмарних ресурсах і центрах обробки даних як джерелах електронних (цифрових) доказів у провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі, зокрема встановлено, що ними є: 1) дані, які зберігаються у хмарних ресурсах надавачів хмарних послуг і центрів обробки даних, що перебувають у володінні надавачів послуг таких центрів; 2) дані про доступ до цієї інформації користувача хмарних послуг або центру обробки даних; 3) дані про наявність резервних копій такої інформації та систем даних і про передання резервних копій інформації користувачу; 4) дані про несанкціоновані дії, спрямовані на доступ до інформації, яка зберігається у хмарному сховищі або центрі обробки даних (існування зовнішніх і

внутрішніх загроз, кібератаки та інциденти кібербезпеки); 5) дані про знищення інформації та її резервних копій;

– запропоновано доповнити КПК України ст. 88^2 під назвою «Допустимість доказів, отриманих із відкритих джерел» та викласти її у такій редакції: «Докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами, які визнані допустимими за правилами цього Кодексу»;

– запропоновано доповнити ч.2 ст. 237 КПК України абз. третім такого змісту: «Під час огляду житла чи іншого володіння особи виявлення та фіксація комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення огляду можлива лише за добровільною згодою володільця цього майна або якщо дозвіл на такий огляд був наданий в ухвалі слідчого судді»;

– запропоновано викласти абзац другий ч.6 ст. 236 КПК України у такій редакції: «Прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що міститься у комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, на місці проведення обшуку виключно якщо дозвіл на такий пошук наданий в ухвалі слідчого судді». Водночас обґрунтовано, що чинна редакція абз. 2 ч.6 статті 236 КПК України може бути застосовною в умовах воєнного стану, коли публічний інтерес розслідування злочинів проти основ національної безпеки превалює над приватним;

– запропоновано доповнити ч.4 ст. 163 КПК України нормою, відповідно до якої клопотання слідчого, прокурора про тимчасовий доступ до речей і документів, що містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо розглядається слідчим суддею у день його надходження;

удосконалено:

– класифікацію електронних (цифрових) доказів, зокрема з урахуванням її теоретичного та практичного значення та із застосуванням логічних правил поділу понять такі докази за критерієм їх форми запропоновано поділяти на наступні види: 1) електронні документи (текстові документи, аудіо- та відеозаписи, фотознімки та інші зображення); 2) електронні повідомлення (текстові, мультимедійні та голосові); 3) віртуальні активи; 4) логи, дані клієнтського середовища, контекстні дані, метадані та інші технічні дані; 5) інша інформація в електронній (цифровій) формі;

– науковий підхід до визначення поняття «кримінальне правопорушення, вчинене у кіберпросторі», під яким запропоновано

розуміти передбачене законом України про кримінальну відповідальність суспільно небезпечне винне діяння, що вчиняється суб'єктом кримінального правопорушення у межах або з використанням кіберпростору як особливого соціально-технічного та інформаційного середовища, шляхом застосування інформаційно-комунікаційних технологій, комп'ютерних систем, мереж чи цифрових даних, та посягає на охоронювані кримінальним законом суспільні відносини;

– науковий підхід до виокремлення мінімальних гарантій захисту права на повагу до приватного та сімейного життя у кіберпросторі відповідно до вимог статті 8 Конвенції та прецедентної практики ЄСПЛ. Зокрема, виокремлено такі гарантії як: 1) чітке законодавче визначення категорій осіб та даних, щодо яких можливе перехоплення; 2) наявність попереднього судового контролю або ефективного подальшого нагляду за спостереженням; 3) нормативне формулювання критеріїв, за якими ухвалюється рішення про ініціювання перехоплення; 4) обмеження строків зберігання даних та встановлення чіткого порядку їх знищення;

– поняття «спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі» під якими запропоновано розуміти сукупність наукових знань і практичних навичок у сфері інформаційних технологій, комп'ютерних систем і мереж, цифрової та комп'ютерно-технічної криміналістики, телекомунікацій, інформаційної безпеки, програмування, аналізу шкідливого програмного забезпечення та електронних фінансових технологій, здобутих у межах академічної підготовки й професійного досвіду, носіями яких є залучені до кримінального провадження за рішенням слідчого, прокурора, слідчого судді чи суду особи, що використовуються з метою вирішення питань, необхідних для повного, всебічного й об'єктивного встановлення фактичних обставин кримінального провадження;

набули подальшого розвитку:

– доктринальні положення щодо розуміння сутності електронних (цифрових) доказів, зокрема на підставі дослідження теоретичних підходів до її розкриття виокремлено процесуальний, технічний і криміналістичний аспекти її розуміння, вказано на взаємодоповнюваність і взаємозв'язок цих аспектів, визначено з їх урахуванням ознаки цих доказів і сформульовано авторську дефініцію їх поняття;

– доктринальні підходи до розуміння поняття та системи джерел електронних (цифрових) доказів, зокрема доведено, що в ході досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі, ними є: 1) електронні пристрої, які містять значиму для кримінального провадження інформацію; 2) електронні комунікаційні системи, які використовувалися в ході підготовки до кримінальних правопорушень у кіберпросторі, їх вчинення та приховування наслідків цих правопорушень;

3) сервери постачальників електронних комунікаційних послуг, хмарні ресурси надавачів хмарних послуг і центри обробки даних надавачів послуг таких центрів;

– наукові підходи до класифікації кримінальних правопорушень, вчинених у кіберпросторі, зокрема, запропоновано здійснювати таку класифікацію залежно від способу реалізації їх об'єктивної сторони;

– підходи до визначення міжнародних процедурних стандартів розслідування кіберзлочинів, які є спільними для усіх регіональних систем захисту прав людини;

– пропозиції щодо нормативного закріплення допустимості проведення зняття інформації з електронних комунікаційних мереж до постановлення ухвали слідчого судді на підставі постанови слідчого, прокурора у випадку, передбаченому ч.1 ст. 250 КПК України.

Оцінка наукового рівня дисертації і наукових публікацій здобувача. Дисертація складається зі вступу, трьох розділів, що включають 9 підрозділів, висновків, списку використаних джерел (205 найменувань) та 3 додатків. Загальний обсяг дисертації складає 201 сторінку, з них основний текст – 171 сторінка, додатки розміщені на 8 сторінках.

Дисертаційне дослідження характеризується логічно побудованим планом та змістом, науково обґрунтованими та вичерпними висновками.

Перший розділ «Теоретико-методологічні основи наукового дослідження проблем доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі» містить чотири підрозділи і присвячений аналізу стану наукової розробленості проблем доказування у кримінальних провадженнях щодо правопорушень, вчинених у кіберпросторі, визначенню поняття кіберпростору та кримінальних правопорушень, що вчиняються у ньому, дослідженню гарантій забезпечення права особи на повагу до приватного життя у кіберпросторі у практиці Європейського суду з прав людини, а також аналізу міжнародних стандартів і зарубіжного досвіду регламентації розслідування кримінальних правопорушень цієї категорії.

Другий розділ «Докази та джерела доказів при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі» містить два підрозділи і присвячений дослідженню теоретичних і практичних аспектів використання електронних (цифрових) доказів у кримінальному провадженні, зокрема визначенню їх поняття, ознак та класифікації, а також аналізу основних джерел електронних (цифрових) доказів, які можуть бути використані під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Третій розділ «Особливості збирання та перевірки доказів при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі» містить три підрозділи і присвячений дослідженню процесуальних та організаційних особливостей збирання і

перевірки доказів у кримінальних провадженнях цієї категорії, зокрема аналізу проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів, а також використання спеціальних знань у сфері інформаційних технологій під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

У **Висновках** викладені основні результати дисертаційного дослідження у вигляді підсумкових суджень, що відповідає вимогам, встановленим для відповідного виду робіт.

Оформлення дисертації відповідає встановленим вимогам.

Усі завдання, які поставив перед собою здобувач для досягнення поставленої мети, вважаю вирішеними.

Основні результати проведених автором наукових досліджень, викладені у дисертаційному дослідженні, належним чином відображені у наукових працях. Основні положення дисертаційного дослідження відображені у дев'яти наукових публікаціях, у тому числі у п'ятьох статтях, опублікованих у наукових фахових виданнях, перелік яких затверджено МОН України, а також чотирьох тезах доповідей на науково-практичних конференціях.

Теоретична та практична значимість результатів дисертаційного дослідження полягає у тому, що сформульовані у дисертації висновки та пропозиції можуть бути використані у: 1) науково-дослідній роботі – для розвитку подальших наукових досліджень проблематики кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі; 2) правотворчій діяльності – для удосконалення нормативної регламентації кримінального процесуального доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі; 3) правозастосовній діяльності – для забезпечення єдності застосування норм кримінального процесуального та суміжного законодавства, що регламентує питання доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі; 4) навчальному процесі – при викладанні навчальних дисциплін «Кримінальний процес», «Сучасні проблеми кримінально-процесуального права», «Проведення слідчих (розшукових) дій», «Оперативно-розшукові заходи та негласні слідчі (розшукові) дії», «Забезпечення законності проведення оперативно-розшукових заходів та слідчих (розшукових) дій»

Дотримання принципів академічної доброчесності.

У дисертаційному дослідженні та/або наукових публікаціях здобувача М.В. Філімонова НЕ виявлено текстових запозичень без посилання на першоджерело, фабрикації, фальсифікації та інших порушень принципів академічної доброчесності. Академічний текст можна вважати авторським і оригінальним у важливій для кримінальної процесуальної науки та

правозастосовної діяльності площині – доказуванні при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі.

Щодо конфлікту інтересів. Рецензент не має реального чи потенційного конфлікту інтересів щодо здобувача, Філімонова Микити Володимировича, його наукового керівника, Хижняка Євгена Сергійовича, та не є їх близькою особою.

Відзначаючи в цілому високий науковий рівень дисертаційного дослідження, його структурно-логічну побудову, наукову новизну, можу зауважити, що ***робота містить низку дискусійних питань та положень, які дозволять ще краще зрозуміти її значення і розкрити зміст теми. Зазначені питання потребують розкриття і додаткової аргументації, зокрема***:

1. В роботі автор пропонує при оцінці допустимості доказів, отриманих з відкритих джерел, обов'язково підтверджувати такі відомості іншими доказами. Для цього пропонується внести зміни до КПК України і доповнити текст Кодексу наступним положенням «докази, отримані із відкритих джерел можуть бути визнані допустимими виключно за умови підтвердження джерела їх походження та якщо відповідні відомості підтверджуються іншими доказами…». В той же час будь-який доказ незалежно від джерела його отримання має підтверджуватись іншими доказами, що власне і відбувається під час перевірки доказів та є фактичним відображенням правила «жоден доказ не має наперед встановленої сили». Тому доцільність нормативного закріплення такого правила конкретно по відношенню до доказів, отриманих з відкрити джерел, виглядає сумнівною.

2. В роботі автор досить слушно зазначає про можливі зловживання з боку сторони обвинувачення під час обшуків в частині проведення несанкціонованого огляду комп'ютерних систем. З метою недопущення таких зловживань автор пропонує внести зміни до ст. 236 КПК України та передбачити, що огляд комп'ютерних систем тощо можливий під час обшуку лише в тому випадку, коли це чітко зазначено в ухвалі. Погоджуючись з автором в частині наявності ризиків зловживання повноваженнями, слід констатувати, що запропонована зміна виглядає дещо радикальною. Обшук часто проходить в умовах невизначеності та потребує від уповноважених осіб коригування поведінки на місці. Власне саме з такою метою законодавець дозволив під час обшуку вилучати всі речі і документи, які можуть мати відношення до кримінального провадження, незалежно від того, чи були вони зазначені в ухвалі. Очевидно, що необхідність проведення огляду комп'ютерних систем може виникати незалежно від попереднього бажання слідчого або прокурора, а неможливість проведення такої процесуально дії може поставити під сумнів результативність всього обшуку. Можливо доцільно в даному випадку застосовувати «наступний» судовий контроль по аналогією з арештом

майна, на вилучення якого не було попереднього дозволу, коли слідчий суддя буде аналізувати законність огляду комп'ютерних систем після того, як вони були проведені.

Звертаю увагу на те, що вказані зауваження і питання не впливають на загальну високу оцінку дисертаційного дослідження, належний рівень виконання, а лише спрямовані на доповнення і кращого з'ясування положень, які виносяться на публічний захист і повинні стати предметом дискусійного обговорення.

ЗАГАЛЬНИЙ ВИСНОВОК

1. Дисертаційне дослідження **Філімонова Микити Володимировича** на тему: **«Особливості доказування при здійсненні досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі»** є комплексною, цілісною, оригінальною та завершеною кваліфікаційною науковою працею, яка містить науково цінні та обґрунтовані висновки щодо реалізації правових положень при закритті кримінального провадження при розслідуванні податкових кримінальних правопорушень.

2. Дисертаційне дослідження відповідає спеціальності 081 – «Право» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами), Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами).

3. Здобувач – Філімонов Микита Володимирович – заслуговує на присудження ступеня доктора філософії за спеціальністю 081 «Право».

<u>Рецензент:</u>
доктор юридичних наук, професор
завідувач кафедри кримінального процесу
Національного університету
«Одеська юридична академія» **Олександр ТОРБАС**