

4. Коновалова В. Е. Версия: концепция и функции в судопроизводстве. Харьков : Консум, 2000. 176 с.
5. Бірюков В.В., Мельникова О.Б., Шехавцов Р.М., Попов І.В. Теорія та практика планування розслідування злочинів: навч. посіб. Луганськ : РІО ЛАВС, 2002. 72 с.
6. Криміналістика : підручник для студ. юрид. спец, вищ. закл. освіти / В.М. Глібоко, А.Л. Дудніков, В.А. Журавель та ін. ; за ред. В.Ю. Шепітька. К.: Вид. дім «Ін Юре», 2001. 684 с.
7. Шило А.І. Методика розслідування хабарництва в контексті нового антикорупційного законодавства України : дис. ... канд. юрид. наук: спец. 12.00.09. К., 2013. 244 с.
8. Пясковський В.В., Чорноус Ю.М., Іщенко А.В., Алексєєв А.А. та ін. Криміналістика : підручник. К. : Центр учбової літератури, 2015. 544 с.

УДК 343.98

DOI <https://doi.org/10.32844/2618-1258.2024.3.42>

ПЕРХУН С.О.

### АКТУАЛЬНІ ПИТАННЯ ПОБУДОВИ АЛГОРИТМІВ ДІЙ УПОВНОВАЖЕНИХ ОСІБ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

#### ACTUAL ISSUES OF BUILDING ALGORITHMS FOR THE ACTIONS OF AUTHORIZED PERSONS DURING THE INVESTIGATION OF FRAUD IN THE FIELD OF INTERNET BANKING USE

Досліджено окремі аспекти розслідування шахрайства у сфері використання інтернет-банкінгу. Розглянуто алгоритми дій працівників правоохоронних органів для вирішення типових слідчих ситуацій у кримінальних провадженнях за фактом учинення досліджуваної категорії кримінальних правопорушень.

Наголошено, що розслідування кримінальних правопорушень має відбуватись у певній послідовності. Ця послідовність забезпечується проведенням процесуальних дій відповідно до типових слідчих ситуацій. Вказана криміналістична категорія виконує роль регулятора реалізації відповідних заходів. Крім того, необхідним є створення відповідних алгоритмів дій працівників правоохоронних органів для їх реалізації.

Сформульовано типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу. Визначено комплекс процесуальних дій під час вирішення першої типової слідчої ситуації розслідування досліджуваного проти-правного діяння: допит потерпілого; встановлення особи шахрая; допит шахрая в статусі підозрюваного; обшук у приміщеннях, де живе або працює шахрай; призначення експертиз.

Обґрунтовано комплекс дій у другій слідчій ситуації, таких як допит потерпілого; огляд місця події з метою виявлення доказів, які допоможуть обмежити коло підозрюваних; тимчасовий доступ до речей і документів; огляд та долучення до справи відеозаписів, фотографій; розшук і встановлення особи шахрая; встановлення особи шахрая; аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі); візуальне спостереження за особою; негласне зняття інформації з транспортних телекомунікаційних мереж; призначення експертиз.

**Ключові слова:** шахрайство, інтернет-банкінг, розслідування, типова слідча ситуація, алгоритми, слідча (розшукова) дія, негласна слідча (розшукова) дія.

The scientific article is devoted to some aspects of the investigation of fraud in the use of Internet banking. Algorithms of actions of law enforcement officers to solve typical investigative situations in criminal proceedings based on the fact of committing the investigated category of criminal offenses are considered.

It is emphasized that the investigation of criminal offenses should take place in a certain sequence. This sequence is ensured by conducting procedural actions in accordance with typical investigative situations. The specified criminalistic category performs the role of a regulator of the implementation of the above measures. In addition, it is necessary to create appropriate algorithms for the actions of law enforcement officers for their implementation.

Typical investigative situations of the investigation of fraud in the field of Internet banking are formulated. A set of procedural actions during the resolution of the first typical investigative situation of the investigation of the investigated illegal act is defined: interrogation of the victim; identification of the fraudster; interrogation of the fraudster as a suspect; search in the premises where the fraudster lives or works; appointment of examinations.

A complex of actions in the second investigative situation is provided, such as: interrogation of the victim; inspection of the scene of the incident in order to identify evidence that will help narrow down the circle of suspects; temporary access to things and documents; review and attachment of video recordings and photographs to the case; search and identification of the fraudster; identification of the fraudster; audio control of a person by installing technical means in a publicly inaccessible place (vehicle, apartment); visual observation of a person; tacit knowledge of information from transport telecommunication networks; appointment of examinations.

**Key words:** *fraud, Internet banking, investigation, typical investigative situation, algorithms, investigative (search) action, covert investigative (search) action.*

**Постановка проблеми.** Розслідування кримінальних правопорушень має відбуватися у певній послідовності. Ця послідовність забезпечується проведенням слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій відповідно до типових слідчих ситуацій. Вказана криміналістична категорія виконує роль регулятора реалізації перелічених заходів. Кримінальні провадження, розпочаті за фактом учинення шахрайства у сфері використання інтернет-банкінгу, також потрібно здійснювати до зазначених ситуацій. Крім того, необхідним є створення відповідних алгоритмів дій працівників правоохоронних органів для їх реалізації.

**Аналіз публікацій, у яких започатковано розв'язання проблеми.** Важливий доробок в опрацювання побудови алгоритмів дій уповноважених осіб під час розслідування різних категорій протиправних діянь зробили такі науковці, як Л. І. Аркуша, В. П. Бахін, В. Д. Берназ, А. Ф. Волобуєв, М. М. Єфімов, В. А. Журавель, В. Г. Лукашевич, Н. В. Павлова, М. А. Погорецький, М. В. Салтєвський, О. А. Самойленко, Р. Л. Степанюк, В. В. Тіщенко, К. О. Чаплинський, С. С. Чернявський, Ю. М. Черноус, В. Ю. Шепітько та ін. У нашій роботі конкретизовано сутність вказаної наукової категорії під час розслідування визначеного виду кримінальних правопорушень з огляду на сучасну судово-слідчу практику та позиції окремих дослідників.

**Метою статті** є дослідження побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу.

**Виклад основного матеріалу.** Результати опрацювання судово-слідчої практики дали змогу сформулювати такі типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу:

- 1) учинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна доказова база, шахрай відомий – 27 %;
- 2) учинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна доказова база, шахрай невідомий – 52 %;
- 3) учинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна та матеріальна доказова база, шахрай невідомий – 16 %;
- 4) учинено шахрайські дії у сфері використання інтернет-банкінгу, повністю відсутня доказова база – 5 %.

З огляду на зазначене, вважаємо за доцільне навести твердження К. Ю. Назаренко, яка зауважувала, що аналіз та оцінка слідчої ситуації мають істотне значення, адже дозволяють

«зорієнтуватись у різноманітні фактів і явищ, які стосуються особи злочинця на момент розслідування; усвідомити наукові знання (рекомендації криміналістики) щодо типових матеріальних джерел (слідів), у яких відбувається подія злочину; опанувати методики та практики пошуку таких джерел, отримати від них належну інформацію, її фіксація та подальше збереження; виконувати практичну роботу з цими джерелами інформації; зіставляти отриману інформацію з даними оперативних і криміналістичних обліків; висунути відповідні версії про місцезнаходження та сліди, що містять інформацію про властивості особи злочинця; визначити найбільш доцільні тактичні прийоми, рекомендації, комбінації зі збирання слідів і встановлення злочинця; вибрати найбільш ефективні техніко-криміналістичні засоби й методи для цих цілей; вибрати найбільш ефективні форми використання спеціальних знань і взаємодії з органами дізнання з метою одержання криміналістично значущої інформації про особу злочинця; вивести з версій слідства; спланувати початковий етап розслідування» [5, с. 82].

Натомість інші дослідники (Н. А Жерж, М. Є. Дирдін) зауважують, що для вирішення визначених ситуацій працівники Національної поліції України зобов'язані реалізувати низку заходів, які акумулюються в певному порядку. Окремі науковці алгоритм дій слідчого в розслідуванні насильницьких злочинів визначають таким чином: аналіз наявної інформації; оцінка вихідної слідчої ситуації, висунення версій за фактичними та ймовірними обставинами подій; постановка тактичних завдань і планування розслідування; проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій і тактичних операцій з перевірки висунутих версій [2, с. 118–119].

Слушною є думка А. В. Рейнгольда, який стверджує, що «...перша слідча ситуація передбачає проведення комплексу заходів, спрямованих на встановлення всіх обставин справи та доведення вини особи, яку підозрюють у вчиненні шахрайства в інтернет-комерції, зокрема: допиту потерпілого щодо обставин здійснення правочину в дистанційній формі та умов, які висувалися продавцем і покупцем; встановлення умов створення сайту, на якому викладалися пропозиції щодо купівлі-продажу товарів і послуг; отримання інформації від інтернет-провайдерів та операторів телекомунікаційного зв'язку; допиту підозрюваного щодо обставин ошукування громадянина, легітимності існування його діяльності тощо; отримання характеризуючих даних про підозрюваного; пред'явлення підозрюваного для впізнання потерпілому (за умов спілкування у відеорежимі); огляд засобів комп'ютерної техніки, проведення обшуку в підозрюваного тощо; призначення комп'ютерно-технічної та інших експертиз тощо» [7, с. 127–128]. Тобто комплекс слідчих (розшукових), негласних слідчих (розшукових) дій та інших процесуальних дій під час вирішення першої типової слідчої ситуації розслідування шахрайства у сфері використання інтернет-банкінгу має такий вигляд:

- допит потерпілого;
- огляд електронно-обчислювальної техніки (далі – ЕОТ) потерпілого (комп'ютера, смартфона, планшета);
- встановлення особи шахрая;
- допит шахрая в статусі підозрюваного;
- обшук у приміщеннях, де живе або працює шахрай;
- вилучення ЕОТ, виявленої під час проведення обшуку (комп'ютер, смартфон, планшет, жорсткі диски);
- призначення експертиз.

Наприклад, з 20 липня 2020 року гр. А. перебував на строковій військовій службі у військовій частині. 23 грудня 2020 року гр. А. вибув на лікування в шпиталь. У період з 26 до 30 грудня 2020 року, ОСОБА\_5, перебуваючи у військовому шпиталі, в інфекційному відділенні, познайомився із військовослужбовцем гр. Д., який також перебував на лікуванні в тому самому відділенні. У спілкуванні гр. А. заручився довірою гр. Б. та в нього виник умисел щодо заволодіння грошовими коштами останнього в сумі 5000 грн. Реалізуюючи його, шахрай під приводом необхідності скористатися мобільним телефоном гр. Д. заволодів належним останньому телефоном з доступом до мобільних додатків. Крім того, продовжуючи свій злочинний намір на заволодіння грошовими коштами гр. Д., повідомив йому, що повинен отримати грошові кошти від матері, однак власну банківську карту залишив у військовій частині та попросив банківську карту гр. В. з пін-кодом до неї, заволодівши таким чином і нею. У подальшому, 30 грудня 2020 року, гр. А., маючи безперешкодний доступ до мобільних додатків мобільного телефону гр. Д., за допомогою кредитного інтернет-банкінгу оформив кредит у ТОВ «Смартвей Юкрейн» на суму 600 грн, поставивши електронний підпис з одноразовим ідентифікатором потерпілого.

Крім того, 30 грудня 2020 року, о 18:18 він за допомогою кредитного інтернет-банкінгу оформив кредит у ТОВ «Манівео швидка фінансова допомога» на суму 2000 грн. Вказані грошові кошти перерахував на банківську картку та здійснив купівлю продуктів у магазинах м. Полтава, користувався кур'єрськими послугами «Glovo» та мобільними інтернет-додатками на суму 2000 грн. Загалом гр. А. заволодів грошовими коштами потерпілого на загальну суму 4750 грн [10]. Надалі шахрая ідентифікували шляхом проведення допитів потерпілих та огляду смартфона потерпілого, де було збережено всі операції інтернет-банкінгу.

Стосовно другої слідчої ситуації слід зауважити, що оскільки особа шахрая невідома, варто розпочинати заходи з його встановлення та розшуку. Щодо розшуку ми цілком поділяємо позицію В. О. Малярвої, яка наголосила на систематичному виконанні таких задач, як виявлення джерел інформації про ознаки шуканого злочинця; побудова гіпотетичної моделі злочинця (особи, яку розшукують) і встановлення його належності до: широкої сукупності (класу) осіб за загальними ознаками; вузької сукупності (групи) осіб за окремими ознаками; встановлення обмеженої, кількісно визначеної групи осіб, що перевіряються; встановлення особи, яку перевіряють, тобто особи, яка згідно з обставинами кримінального провадження може бути шуканим злочинцем, та за потреби отримання від неї зразків для експертизи, відповідно до ст. 245 КПК України; ідентифікація конкретної особи; встановлення шуканого злочинця [4, с. 131]. Тобто в другій слідчій ситуації варто проводити такі заходи:

- допит потерпілого;
- огляд місця події з метою виявлення доказів, які допоможуть обмежити коло підозрюваних;
- огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета);
- тимчасовий доступ до речей і документів;
- огляд та долучення до справи відеозаписів, фотографій;
- розшук і встановлення особи шахрая;
- встановлення особи шахрая;
- аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі);
- візуальне спостереження за особою;
- негласне зняття інформації з транспортних телекомунікаційних мереж;
- призначення експертиз.

Крім того, Т. В. Коршикова доречно вказувала, що «...для перевірки слідчих версій, які можуть висуватися за результатами аналізу IP-адрес, за якими використовували ЕОТ з метою вчинення шахрайства для вчинення шахрайства використовували: 1) одну IP-адресу; 2) декілька IP-адрес; 3) невстановлені IP-адреси» [3, с. 369]. Як бачимо, обов'язковим є аналіз IP-адрес, за якими здійснювалось використання ЕОТ з метою вчинення шахрайства, що є передумовою ефективного розслідування досліджуваної категорії кримінальних правопорушень.

Натомість А. В. Рейнгольд наголошував, що слід спрямувати всі зусилля на дослідження: операційної системи та оперативної пам'яті; вивчення змісту файлів; web-браузерів; вивчення змісту електронної пошти; вивчення змісту смс-повідомлень, журналу вхідних і вихідних дзвінків на мобільному пристрої потерпілого тощо [8, с. 131].

Також, як доречно зауважила Г. В. Захарова, слід докладно допитати потерпілого та свідків щодо прикмет особи, яка вчинила шахрайство, скласти та поширити орієнтування, повідомити інформацію про злочинця в засоби масової інформації тощо. Інформацію про місцезнаходження шахрая можуть надати його знайомі та родичі, співробітники й інші особи. Оперативним працівникам можна здійснити спостереження за місцями можливої появи шахрая та за потреби здійснити зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем. Водночас слід пам'ятати, що ці заходи є негласними слідчими (розшуковими) діями та можуть проводитися лише за дорученням слідчого на підставі ухвали слідчого судді (за умови вчинення злочину, а не проступку). Якщо шахрайство кваліфікуватиметься за ч. 1 ст. 190 КК України, це буде кримінальний проступок і серед усіх негласних слідчих (розшукових) дій можна проводити лише дві: встановлення місцезнаходження радіоелектронного пристрою та зняття інформації з електронних інформаційних систем (без порушення системи логічного захисту). Докази щодо дійсного злочинного наміру можна отримати не лише зі свідчень потерпілих і свідків обставин шахрайських дій, а й під час огляду документів, електронних інформаційних носіїв, уважно оглядаючи відповідні інформаційні ресурси, сервіси в мережі Інтернет, зокрема вебсайти, на яких міститься інформація, що може допомогти довести дійсно злочинний намір

шахраїв. З цією метою доцільно проводити й негласні слідчі (розшукові) дії, знімаючи необхідну інформацію з каналів зв'язку» [1, с. 145].

Водночас інші науковці (Н. В. Павлова, Д. А. Птушкін, К. О. Чаплинський) доводять, що в ситуації, коли особистість шахрая невідома, проводять комплекс розшукових заходів з використанням словесного й композиційного портретів. Зі слів потерпілих і свідків за прикметами шахраїв складають суб'єктивні портрети, перевіряють за обліками сліди пальців рук, виявлені на документах і предметах. Корисним може бути й вивчення практики застосування аналогічних способів шахрайства за архівними кримінальними справами (провадженнями) [6, с. 65].

Наприклад, у середині листопада 2016 року гр. О. вступив у попередню змову з гр. З. та вчинив низку заволодінь чужим майном шляхом обману через незаконні операції з використанням ЕОТ. У вказаний час шахрай зі своїм подільником з використанням невстановленої комп'ютерної техніки шляхом реєстрації інтернет-сайтів з відповідними назвами доменних імен створив низку «фейкових» інтернет-магазинів, зокрема: <http://technobox.net.ua>, <http://mobilook.com.ua>, <http://technolab.in.ua>, <http://technomart.net.ua>, <http://supersmart.in.ua>, <http://mobiliti.net.ua>, <http://mobiland.net.ua>, <http://technoplaza.net.ua>, <http://evoshop.com.ua>, <http://mobilson.com.ua>. Вказані фейкові платформи спеціалізувалися на реалізації мобільних телефонів. Оформлення сайтів, порядок їх функціонування, а також розміщення інформації з повним технічним описом товару не викликали в покупців сумнівів у реальності існування магазинів. Крім того, гр. О. разом зі своїм співучасником з метою залучення якомога більшої кількості осіб, що зацікавлені в розміщенні на інтернет-сайтах товаром, у невстановлений досудовим розслідуванням час виклав завідомо неправдиву інформацію про продаж мобільних телефонів торгових марок «Apple», «Xiaomi», «Meizu», «Samsung» та інших популярних виробників, вказуючи значно нижчу вартість товару, що продається, ніж пропонують інші продавці. Також з метою підняття рейтингів і пошукової конкурентоспроможності (SEO-показники), які б дозволили за будь-якого пошукового запиту користувача мережі Інтернет щодо купівлі мобільних телефонів видавати його інтернет-магазин серед перших для потенціальних покупців, гр. О. разом зі своїм співучасником використовував послуги інтернет-майданчика «<http://price.ua>», який дозволяв видавати для потерпілих порівняльну з іншими інтернет-магазинами інформацію та показував, що ціна товару в його інтернет-магазині є значно нижчою, ніж в інших магазинах. У подальшому шахрай переводив у готівку сплачені клієнтами «фейкових» магазинів грошові кошти через мережу банкоматів, розташованих як на території м. Дніпро, так і в окремих районах і містах Дніпропетровської області. Під час користування банкоматами гр. О. з метою уникнення фіксації камер відео- та фотоспостереження, які розташовані в банкоматах і на прилеглих територіях, з метою подальшого унеможливлення ідентифікації своєї особи одягав на обличчя заздалегідь підготовлену маску. Заволодівши в такий спосіб грошовими коштами потерпілих, шахраї розпоряджались ними на власний розсуд [9]. У процесі розслідування наведеного факту шахрайства у сфері використання інтернет-банкінгу уповноважені особи реалізували майже весь комплекс процесуальних дій і заходів, визначених нами в другій типовій слідчій ситуації: починаючи з допиту потерпілих і закінчуючи проведенням аудіоконтролю гр. О. шляхом встановлення технічних засобів у публічно недоступному місці (у його транспортному засобі «Toyota Camry»), візуальним спостереженням за ним і негласним зняттям інформації з транспортних телекомунікаційних мереж. Завдяки максимально ефективному здійсненню всіх вказаних заходів особу було затримано, а в подальшому винесено обвинувальний вирок у вчиненні кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України.

**Висновки.** Підбиваючи підсумки, зазначимо, що розслідування кримінальних правопорушень має відбуватись у певній послідовності. Проведене дослідження дало змогу сформулювати типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу, а також визначити комплекс процесуальних дій під час вирішення першої типової слідчої ситуації розслідування досліджуваного протиправного діяння, зокрема: допит потерпілого; огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета); встановлення особи шахрая; допит шахрая в статусі підозрюваного; обшук у приміщеннях, де живе або працює шахрай; вилучення ЕОТ, виявленої під час проведення обшуку (комп'ютер, смартфон, планшет, жорсткі диски); призначення експертів. Доречним є такий комплекс дій у другій слідчій ситуації: допит потерпілого; огляд місця події з метою виявлення доказів, які допоможуть обмежити коло підозрюваних; огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета); тимчасовий доступ до речей і документів; огляд і допущення до справи відеозаписів, фотографій; розшук і встановлення особи шахрая; встановлення особи шахрая; аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі); візуальне спостереження за особою; негласне зняття інформації з транспортних телекомунікаційних мереж; призначення експертів.



**Список використаних джерел**

1. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою : дис. ... канд. юрид. наук : 12.00.09. Київ, 2021. 246 с.
2. Жерж Н. А., Дирдін М. Є. Слідчі ситуації та типові криміналістичні версії щодо особи злочинця при розслідуванні окремих насильницьких злочинів. *Науковий вісник Ужгородського національного університету*. 2015. Вип. 32. Т. 3. С. 117–121.
3. Коршикова Т. В. Алгоритм дій слідчого з розслідування шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні питання криміналістики : матеріали Всеукр. наук.-практ. конф. (Київ, 20 груд. 2019 р.) / редкол. : В. В. Черней, С. Д. Гусарев, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2019. С. 368–370.*
4. Малярова В. О. Тактико-криміналістичні та процесуальні основи пошуку та затримання злочинця : дис. ... канд. юрид. наук : 12.00.09. Харків, 2005. 238 с.
5. Назаренко К. Ю. Розслідування злочинів, пов'язаних зі створенням або утриманням місць розпусти і звідництвом : дис. ... канд. юрид. наук : 12.00.09. Дніпро, 2016. 218 с.
6. Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов'язаного з відчуженням об'єктів нерухомого майна громадян : монографія. Херсон : Гельветика, 2019. 196 с.
7. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. ... канд. юрид. наук : 12.00.09. Дніпро, 2023. 250 с.
8. Рейнгольд А. В. Типові слідчі ситуації під час розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 2. Т. 2. С. 129–133.
9. Справа № 200/12729/18. Архів Бабушкінського районного суду м. Дніпропетровська, 2021 р.
10. Справа № 554/1839/21. Архів Октябрського районного суду м. Полтави, 2021 р.

УДК 343

DOI <https://doi.org/10.32844/2618-1258.2024.3.43>

**ТИМОЩУК С.О.**

**ПРОВЕДЕННЯ НЕГЛАСНОЇ СЛІДЧОЇ (РОЗШУКОВОЇ) ДІЇ ДО ПОСТАНОВЛЕННЯ УХВАЛИ СЛІДЧОГО СУДДІ: ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ**

**CONDUCTING AN COVERT INVESTIGATIVE (SEARCH) ACTION BEFORE THE DECISION OF THE INVESTIGATING JUDGE: PROBLEMS AND WAYS TO SOLVE THEM**

У статті дотримана наукова позиція щодо безальтернативної можливості розпочинати проведення у кримінальному провадженні за рішенням слідчого, узгодженого з прокурором, або прокурора у випадках, визначених ч. 1 ст. 250 Кримінального процесуального кодексу України, лише двох негласних слідчих (розшукових) дій – установлення місцезнаходження радіообладнання (радіоелектронного засобу) та спостереження за особою. Доведено, що зазначені правові норми повною мірою взаємопов'язані та узгоджуються між собою, що не дає жодних підстав трактувати сферу практично-правового застосування правового інституту «Проведення негласної слідчої (розшукової) дії до постановлення ухвали слідчого судді» в іншій правовій площині.

---

© ТИМОЩУК С.О. – аспірант наукової лабораторії з проблем протидії злочинності (Навчально-науковий інститут № 1 Національної академії внутрішніх справ)