

В. С. Бабкова,

кандидат юридичних наук, доцент, доцент кафедри судоустрою та прокурорської діяльності Національного юридичного університету імені Ярослава Мудрого

ПРОБЛЕМИ ВИЗНАННЯ РЕЗУЛЬТАТІВ ЗНЯТТЯ ІНФОРМАЦІЇ З ТРАНСПОРТНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НАЛЕЖНИМИ ТА ДОПУСТИМИМИ ДОКАЗАМИ

Анотація. У науковій статті розглядаються питання визнання доказами результатів зняття інформації з транспортних телекомунікаційних мереж. Аналізуються проблеми відповідності таких доказів вимогам належності та допустимості. Обґрунтовується висновок про необхідність проведення фоноскопичної експертизи для визнання результатів цієї негласної слідчої (розшукової) дії належними і допустимими доказами

Ключові слова: докази, доказування, належність доказів, допустимість доказів, зняття інформації з транспортних телекомунікаційних мереж.

Аннотация. В научной статье рассматриваются вопросы признания доказательств результатов снятия информации с транспортных телекоммуникационных сетей. Анализируются проблемы соответствия таких доказательств требованиям относимости и допустимости. Обосновывается вывод о необходимости проведения фоноскопической экспертизы для признания результатов этого негласного следственного (розыскного) действия относимыми и допустимыми доказательствами.

Ключевые слова: доказательства, доказывание, относимость доказательств, допустимость доказательств, снятие информации с транспортных телекоммуникационных сетей.

Summary. In the scientific article questions of recognition are considered by proofs of results of removal of information from transport telecommunication networks. Problems of compliance of such proofs to requirements of relevancy and admissibility are analyzed. A conclusion about need of conducting phonoscope examination for recognition of results of this secret investigative (search) action is proved by the carried and admissible proofs.

Key words: proofs, proof, relevancy of proofs, admissibility of proofs, removal of information from transport telecommunication networks.

Постановка проблеми. У теорії кримінального процесу властивостями будь-якого доказу вважаються належність, допустимість, достовірність, а сукупності доказів – їх достатність. Лише наявність всіх цих ознак дозволяє використовувати конкретні фактичні дані як докази у кримінальному провадженні. Разом із тим за провадження у вітчизняний кримінальний процес нових інститутів та ускладнення процесуальної діяльності зумовлюють необхідність урахування цих новацій з точки зору процесу доказування, що зумовлює актуальність обраної теми наукової публікації.

© Бабкова В. С., 2018

Аналіз досліджень і публікацій. Проблеми доказування у кримінальному провадженні досліджувалися в роботах таких вітчизняних науковців, як Ю. Грошевий, М. Жогін, О. Капліна, В. Фаринник та ін. Питання зняття інформації з транспортних телекомунікаційних мереж розглядали І. Маскалюк, О. Меживой, М. Самбор, В. Уваров та ін. Водночас, зважаючи на складність та багатоаспектність досліджуваної проблематики, питання визнання доказами результатів зняття інформації з транспортних телекомунікаційних мереж потребують подальшого наукового дослідження.

Зважаючи на це, **метою** наукової статті є встановлення критеріїв визнання належними і допустимими доказами результатів зняття інформації з транспортних телекомунікаційних мереж.

Виклад основного матеріалу. Легальне визначення поняття належності і допустимості доказів закріплено у КПК України. Крім того, воно уточнюється і деталізується у кримінальній процесуальній доктрині. Так, згідно із ст. 85 КПК України, належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню в кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів.

В основу належності доказів покладені об'єктивні зв'язки (причинно-наслідкові, умовно-обумовлені, просторово-часові тощо) між предметами і явищами дійсності. При цьому властивість належності становить логічне відображення будь-якого роду зв'язків. Це – здатність одержуваної інформації бути аргументом у ланцюзі умовиводів, що обґрунтовують наявність або відсутність шуканих фактів. З цієї точки зору неналежними будуть докази, що містять відомості не про досліджувану подію, а про інший факт, що не входить до обставин, які підлягають доказуванню [1, с. 185].

Вирішення питання про належність доказу передбачає дослідження двох моментів. По-перше, чи входить факт, для встановлення якого застосовується певний доказ, до предмета доказування або в число проміжних та інших допоміжних фактів, з'ясування яких необхідно при перевірці версій та доказів. По-друге, чи здатний доказ, з урахуванням його змісту, цей факт встановлювати [2, с. 247].

Регламентуючи питання щодо допустимості доказів, КПК України у ст. 86 встановлює, що доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом. У науковій юридичній літературі допустимість доказів розглядається як отримання доказу в порядку, встановленому законом (з належного джерела, належним суб'єктом, з додержанням встановленої процесуальної форми) [3, с. 130]. На думку Н. В. Сібільової, виявлення властивості допустимості доказів охоплює оцінку: а) відповідності джерела фактичних даних вимогам КПК; б) правомочностей суб'єкта кримінально-процесуальної діяльності на процесуальне закріплення доказів установленим в законі способом, а також законності та етичності використаних тактичних прийомів [4, с. 23].

Стаття 86 КПК України закріплює критерії недопустимості доказів, пов'язуючи це із випадками істотного порушення прав і свобод людини. Згідно із положеннями цієї статті, недопустимими є докази, отримані внаслідок істотного порушення прав та свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також

будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав та свобод людини. Суд зобов'язаний визнати істотними порушеннями прав людини й основоположних свобод, зокрема, такі діяння: 1) здійснення процесуальних дій, які потребують попереднього дозволу суду, без такого дозволу або з порушенням його суттєвих умов; 2) отримання доказів унаслідок катування, жорстокого, нелюдського або такого, що принижує гідність особи, поводження або погрози застосування такого поводження; 3) порушення права особи на захист; 4) отримання показань чи пояснень від особи, яка не була повідомлена про своє право відмовитися від давання показань та не відповідати на запитання, або їх отримання з порушенням цього права; 5) порушення права на перехресний допит. Недопустимими є також докази, що були отримані: 1) з показань свідка, який надалі був визнаний підозрюваним чи обвинуваченим у цьому кримінальному провадженні; 2) після початку кримінального провадження шляхом реалізації органами досудового розслідування чи прокуратури своїх повноважень, не передбачених цим Кодексом, для забезпечення досудового розслідування кримінальних правопорушень.

Зняття інформації з транспортних телекомунікаційних мереж, згідно із п. 3 ч. 4 ст. 258 КПК України, є одним із різновидів втручання в приватне спілкування. Відповідно, на проведення цієї процесуальної дії поширюються загальні гарантії втручання у приватне спілкування, передбачені ст. 258 КПК України. Крім того, процесуальний порядок зняття інформації з транспортних телекомунікаційних мереж врегульовано ст. 263 КПК України. Детальна нормативна регламентація цієї процесуальної дії міститься в Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні від 16.11.2012 № 114/1042/516/1199/936/1687/5 [5] (далі – Інструкція).

Ця процесуальна дія полягає у проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку. Аналіз нормативно-правових актів кримінально-процесуального, оперативного-розшукового та телекомунікаційного законодавства, дозволяє стверджувати, що даній негласній слідчій (розшуковій) дії притаманні такі властивості: пов'язана з тимчасовим обмеженням конституційних прав громадян, а саме втручанням у приватне спілкування громадян; здійснюється щодо тяжких або особливо тяжких злочинів у випадках, якщо іншим шляхом отримати інформацію з метою розслідування злочину неможливо; проводиться за ухвалою слідчого судді після погодження з прокурором; полягає в застосуванні спеціальних технічних засобів негласного отримання інформації; тактика проведення аналогічна тактиці проведення оперативного-розшукових заходів із застосуванням технічних засобів негласного отримання інформації; полягає у спостереженні (контролі), відборі інформації, фіксації змісту інформації, а також одержанні, перетворенні та фіксації сигналів, що передаються каналами зв'язку; безпосереднє проведення покладається на уповноважені оперативно-технічні підрозділи; передбачає отримання інформації, що передавалася особою за допомогою технічних засобів телекомунікацій або каналами зв'язку та має значення для розслідування; може бути проведена як у комплексі з іншими негласними слідчими (розшуковими) діями, так і окремо; передбачає отримання даних про

взаємоз'єднання телекомунікаційних мереж, що дозволяє одночасно встановити місцезнаходження радіоелектронного засобу; результати цієї дії можуть використовуватися у доказуванні на тих самих підставах, що й результати проведення інших слідчих (розшукових) дій [6, с. 232].

Також з положень ст. 263 КПК України можна дійти висновку, що зняття інформації з транспортних телекомунікаційних мереж є різновидом втручання у приватне спілкування, яке проводиться за таких умов: 1) без відома осіб, які використовують засоби телекомунікацій для передавання інформації; 2) на підставі ухвали слідчого судді. При цьому в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування; 3) якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження; 4) покладається на уповноважені підрозділи органів Національної поліції та органів безпеки.

Результатом зняття інформації з транспортних телекомунікаційних мереж, на думку дослідників, є закріплені у формі протоколу про проведення зазначеної негласної слідчої дії фактичні дані, які складають зміст сигналів, що передаються каналами зв'язку, отримані внаслідок застосування відповідних технічних засобів, на підставі яких можна встановити наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [7, с. 203]. Згідно із ч. 1 ст. 265 КПК України, зміст інформації, що передається особами через транспортні телекомунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення зазначених негласних слідчих (розшукових) дій. Однак необхідно звернути увагу на те, що в цій статті та інших положеннях КПК України жодним чином не регламентується ані порядок, ані суб'єкти складення такого протоколу. Зважаючи на це, у науковій юридичній літературі звертається увага на проблему оформлення результатів зняття інформації з транспортних телекомунікаційних мереж протоколом. Її сутність полягає у тому, що згідно з п. 4.1. Інструкції протокол про хід і результати проведеної негласної слідчої (розшукової) дії (або її етапів) складається слідчим, якщо вона проводиться за його безпосередньої участі, в інших випадках – уповноваженим працівником оперативного підрозділу, і повинен відповідати загальним правилам фіксації кримінального провадження. З цього випливає таке: 1) зняття інформації з транспортних телекомунікаційних мереж проводиться оперативно-технічним підрозділом Національної поліції чи СБУ; 2) протокол про проведення зняття інформації з транспортних телекомунікаційних мереж складається оперативним підрозділом, який на підставі свого завдання залучав оперативно-технічний підрозділ Національної поліції чи СБУ, або слідчим, які взагалі не проводили відповідну негласну слідчу (розшукову) дію й не брали участі у ній.

Отже, на думку дослідників, практика фіксації перебігу й результатів негласних слідчих (розшукових) дій слідчим, який безпосередньою участю у її проведенні не брав, не відповідає загальним правилам фіксації кримінального провадження, передбаченим чинним КПК України. Це може призвести до наявності реальних можливостей зловживань, фальсифікації доказів, порушень прав і свобод людини [8, с. 214]; може

мати негативні наслідки при визнанні протоколів про перебіг і результати проведеної негласної слідчої (розшукової) дії (або її етапів) доказами в суді та ускладнити залучення до кримінального процесу осіб, які брали участь у проведенні відповідної негласної слідчої (розшукової) дії як свідки [9, с. 275]; ставить питання щодо допустимості отриманих фактичних даних і можливості визнання їх слідчим, прокурором, слідчим суддею, судом конкретним доказом у кримінальному провадженні [10, с. 37]. Отже, в оцінках ряду дослідників передбачений Інструкцією порядок оформлення результатів зняття інформації з транспортних телекомунікаційних мереж є неналежним та створює підстави для визнання доказів, отриманих таким шляхом, недопустимими.

При цьому ч. 2 ст. 263 КПК України встановлює, що в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування. Такими ідентифікаційними ознаками можуть бути: номер абонента в телефонній мережі загального користування у форматі «код країни – код зони або оператора – номер абонента в мережі»; міжнародний ідентифікаційний номер мобільного терміналу (IMEI); міжнародний ідентифікаційний номер мобільного абонента (IMSI) [11, с. 37].

Найголовніше значення при цьому має унікальна ідентифікація саме абонента спостереження. На думку дослідників, перед прийняттям рішення про зняття інформації з транспортних телекомунікаційних мереж потрібно встановити кількість абонентських номерів, які використовує особа, а також наскільки вона довіряє даному виду зв'язку. Крім того, необхідно звернути увагу на те, що особа може бути не єдиним користувачем телекомунікаційної мережі (абонентського номера) [12, с. 336].

Проте її у разі проведення вказаної негласної слідчої (розшукової) дії забезпечити фактично неможливо. Як зауважують фахівці, ідентифікаційна телекомунікаційна картка, яка використовується для ідентифікації кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо), не дає можливості ідентифікувати абонента – фізичну особу, яка користується такою карткою, адже на сьогодні в Україні немає законодавчої вимоги щодо укладення договору про надання послуг рухомого (мобільного) зв'язку у письмовій формі, що гарантуватиме ідентифікацію абонента [13, с. 180]. Крім того, законодавством України не врегульовано вторинний ринок, на якому здійснюється реалізація ідентифікаційних телекомунікаційних карток, зокрема тому, що договори про надання послуг рухомого (мобільного) зв'язку не підлягають обов'язковій державній реєстрації.

Таким чином, слід зробити висновок про те, що кримінальне процесуальне законодавство України, дозволяючи слідчому, прокуророві чи за їх дорученням уповноваженим оперативним підрозділам проводити відповідно до ст. 263 КПК України негласні слідчі (розшукові) дії, не визначило порядок співвідношення (ідентифікації) кінцевого обладнання з абонентом, адже користуватися кінцевим обладнанням може не лише сам фігурант, а й члени його сім'ї, які, до речі, також можуть користуватися відповідним обладнанням, призначеним для з'єднання

з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг. Виходячи з цього, фактично проведення цієї негласної слідчої (розшукової) дії співвідноситься не стільки з абонентом, скільки з кінцевим обладнанням, відсуваючи на другий план особу, стосовно якої проводяться негласні слідчі (розшукові) дії. Виходячи з цього, формулюється висновок про те, що на сьогодні у слідчого, прокурора чи оперативних підрозділів відсутні практичні можливості надати слідчому судді відомості, які унікально ідентифікують абонента спостереження [14, с. 76–77].

Також у науковій юридичній літературі вказується на негативні випадки, коли в матеріалах кримінального провадження відсутні будь-які об'єктивні дані про належність особі та використання нею номера мобільного телефона. При цьому слідчий, прокурор не завжди вживають заходів і щодо підтвердження даних про користування особою саме вказаним у клопотанні телефоном на момент внесення клопотання до суду, не зазначається інформація, яка є в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості [15, с. 257].

Таким чином, необхідно визнати, що у конкретному випадку зняття інформації з транспортних телекомунікаційних мереж необхідно забезпечити повну ідентифікацію особи. Проте зробити це лише за допомогою ідентифікації певного телекомунікаційного обладнання неможливо. У такій ситуації завжди залишається імовірність того, що телекомунікаційне обладнання використовував не особисто підозрюваний, обвинувачений, навіть якщо на належність йому такого обладнання вказують матеріали справи, а інша особа. Інформація, що в такому разі була предметом зняття, може не належати до особи підозрюваного, обвинуваченого та/або не входить до предмета доказування. Тобто отримані в такий спосіб докази не можуть визнаватися належними і допустимими.

Зважаючи на викладене, слід погодитися із думкою тих дослідників, які вважають, що використанню для доказування матеріалів звукозапису телефонних розмов має передувати експертиза матеріалів і засобів звукозапису, яка може дати відповіді на такі питання: кому з числа перерахованих осіб належать окремі вислови, що містяться на фонограмі; чи є голос, зафіксований на фонограмі, голосом конкретної особи; чи зазнавала змін ця фонограма; чи мають місце ознаки монтажу фонограми; які є ознаки механічного й електронного монтажу фонограми; чи велася зафіксована на фонограмі розмова телефоном тощо. При цьому в науковій юридичній літературі зазначається, що труднощі виникають із матеріалами звукозапису, виготовлених із використанням цифрової техніки. Експерти досі не мають технічної можливості встановити наявності або відсутності ознак монтажу. Якщо експерти роблять висновок про те, що встановити наявності або відсутності ознак монтажу неможливо, зафіксовані на відповідному носії дані стають сумнівними. Усі сумніви мають глумачитися на користь обвинуваченого. А отже, матеріали технічного документування, щодо яких виникають сумніви щодо їх допустимості у справі і достовірності, використанню для доказування не підлягають [16, с. 123–124].

Таким чином, видається, що для ідентифікації особи при знятті інформації з транспортних телекомунікаційних мереж необхідним є проведення фоновскопичної експертизи. Така експертиза проводиться для ідентифікації людини за голосом,

ототоження звукозаписних апаратів і перевірки дійсності фонограми. Експертно-криміналістичне дослідження фонограм включає вивчення звукової інформації, носіїв запису, апаратури і пристосувань, за допомогою яких здійснюється процес запису. Фоноскопична експертиза розвивається в декількох напрямках: технічне дослідження фонограм і інших засобів звукозапису; фоноскопичне дослідження звукового середовища, зафіксованого на магнітних носіях; фоноскопичне дослідження усного мовлення [17, с. 261].

За результатами фоноскопичної експертизи можна отримати відповіді на такі питання: 1. Чи саме на даному технічному апараті зафіксовані фонограма і її фрагменти? 2. Одне чи кілька технічних пристроїв фіксували конкретні фрагменти фонограми? 3. Оригінальна дана фонограма або це копія? 4. Запис фонограми здійснювався без перерв? 5. Чи змінювалася дана фонограма? 6. Одне чи кілька технічних пристроїв фіксували певні фрагменти відеофонограми/фонограми? 7. Які фонограми містять область видаленої інформації технічного пристрою? 8. Чи є можливість відновити в повному обсязі/частково фонограму зі змінного носія інформації? 9. Чи брали певні люди участь у розмові, зафіксованій на фонограмі, і які саме слова та фрази ними промовлені? 10. Яка кількість осіб брала участь у розмові, зафіксованій на аудіозаписі?

Отже, лише за результатами фоноскопичної експертизи можна зробити висновок про те, чи належить голос на фонограмі певній особі.

На підставі викладеного можна зробити такі **висновки**:

1. З огляду на специфіку такої негласної слідчої (розшукової) дії, як зняття інформації з транспортних телекомунікаційних мереж, що являє собою різновид втручання у приватне спілкування, одержана в результаті її проведення інформація з точки зору використання її як доказу в кримінальному провадженні може бути поставлена під сумнів стосовно її належності та допустимості.

2. Оформлення результатів зняття інформації з транспортних телекомунікаційних мереж здійснюється протоколом, який складається оперативним співробітником оперативного підрозділу або слідчим. Проте для визнання зафіксованої у ньому інформації допустимим доказом необхідно встановити, чи брала особисту участь відповідна службова особа у проведенні такої негласної слідчої (розшукової) дії, як зняття інформації з транспортних телекомунікаційних мереж. Складання такого протоколу службовою особою, яка особистої участі у проведенні відповідної процесуальної дії не брала, може розглядатися як передумова визнання цього доказу недопустимим.

3. Використання результатів зняття інформації з транспортних телекомунікаційних мереж як доказів у кримінальному провадженні вимагає встановлення ідентифікаційних ознак, які, зокрема, дозволяють унікально ідентифікувати абонента спостереження. Проте фактично при проведенні цієї негласної слідчої (розшукової) дії здійснюється ідентифікація засобів зв'язку (передання та отримання інформації), а не самого абонента. З огляду на це отримані в результаті зняття інформації з транспортних телекомунікаційних мереж докази можуть виявитися неналежними і недопустимими. Тому для їх підтвердження існує необхідність у ідентифікації особи за фізичними параметрами голосу, яка здійснюється в результаті проведення фоноскопичної експертизи.

Список використаних джерел

1. Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін. ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.
2. Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. Изд. 2-е испр. и доп. Москва : Юрид. лит., 1973. 735 с.
3. Лапкін А. В. Судове право України : навч. посіб. у схемах. 2-ге вид., змін. та допов. Харків : Право, 2017. 150 с.
4. Сибилева Н. В. Допустимость доказательств в советском уголовном процессе : учеб. пособие. Київ : УМК ВО, 1990. 68 с.
5. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. спільним наказом Генеральної прокуратури України, МВС України, СБ України, Міністерством фінансів України, Адміністрацією ДПС України та Міністерством юстиції України № 114/1042/516/1199/936/1681/51 від 16.11.2012. URL: <http://zakon4.rada.gov.ua/laws/show/v0114900-12> (дата звернення: 09.11.2018).
6. Меживой О. В. Правова кваліфікація та регламентація зняття інформації з транспортних телекомунікаційних мереж за новим КПК України. *Вісник Донецького національного університету. Сер. В: Економіка і право*. 2013. Вип. 1. С. 229–233.
7. Єськов С. В. Зняття інформації з транспортних телекомунікаційних мереж як різновид втручання у приватне спілкування: системно-структурний аналіз. *Ученые записки Таврического национального университета им. В. И. Вернадского. Серия «Юридические науки»*. Т. 26 (65). 2013. № 1. С. 199–204.
8. Сергеева Д. Проблемні аспекти використання результатів зняття інформації з транспортних телекомунікаційних мереж як доказів у кримінальному провадженні. *Право України*. 2014. № 11. С. 209–218.
9. Погорецький М. А. Негласні слідчі (розшукові) дії: проблеми провадження та використання результатів у доказуванні. *Юридичний часопис Нац. акад. внутр. справ*. 2013. № 1. С. 270–277.
10. Іскендеров Е. Ф. Зняття інформації з транспортних телекомунікаційних мереж як засіб отримання доказів оперативними підрозділами. *Вісник кримінального судочинства*. 2016. № 4. С. 33–39.
11. Мельник Д. Перспективи нормативно-правового врегулювання зняття інформації з телекомунікаційних мереж та електронних інформаційних систем у новому КПК України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2012. Вип. 2 (24). С. 34–40.
12. Шевченко В. М. Зняття інформації з транспортних телекомунікаційних мереж як оперативно-розшуковий захід, який проводиться при розслідуванні та розкритті корупційних діянь в органах судової влади України. *Часопис Київського університету права*. 2013. № 3. С. 336–339.
13. Самбор М. Договір про надання послуг рухомого (мобільного) зв'язку: до постановки проблеми. *Право України*. 2012. № 7. С. 175–183.
14. Самбор М. Негласні слідчі (розшукові) дії, пов'язані із зняттям інформації з транспортних телекомунікаційних мереж та встановленням місцезнаходження радіоелектронного засобу: підстави для проведення та умови гарантування прав і свобод людини та громадянина як споживача послуг рухомого (мобільного) зв'язку. *Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія «Юридичні науки»*. 2013. № 1 (4). С. 74–81.
15. Маскалюк І. І. Зняття інформації з транспортних телекомунікаційних мереж як різновид втручання у приватне спілкування. *Науковий вісник публічного та приватного права*. 2016. Вип. 4. С. 254–258.
16. Уваров В. Г. Зняття інформації з телекомунікаційних мереж. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 2. Т. 1. С. 121–124.
17. Плахотіна В. М. Призначення й провадження деяких видів експертиз на початковому етапі розслідування хабарництва, вчиненого співробітниками правоохоронних органів. *Актуальні проблеми держави і права*. С. 260–266.