УДК 343.132.5

О. А. Панасюк,
магістр права, адвокат;
С. В. Рак,
канд. юрид. наук, науковий співробітник Лабораторії досліджень проблем національної безпеки у сфері громадського здоров'я Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, асистент кафедри кримінального права та кримінально-правових дисциплін Полтавського юридичного інституту Національного юридичного університету імені Ярослава Мудрого;
Ю. М. Булгакова,
адвокат

ОКРЕМІ ПИТАННЯ НАЛЕЖНОЇ ПРАВОВОЇ ПРОЦЕДУРИ ЗДІЙСНЕННЯ ДОСТУПУ ДО ПРИВАТНОЇ ІНФОРМАЦІЇ ПІД ЧАС ПРОВАДЖЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ

У статті розглянуто окремі проблеми здійснення доступу до приватної інформації під час провадження досудового розслідування кримінальних правопорушень. Правовий захист персональних даних та права на приватне спілкування досліджено в розрізі особливостей здійснення слідчих, негласних слідчих (розшукових), а також інших процесуальних дій у кримінальному провадженні, пов'язаних із доступом до окремих засобів телекомунікації.

***Ключові слова**: захист права на приватність, втручання в приватне спілкування, засоби телекомунікації, негласні слідчі (розшукові) дії, допустимість доказів, належна правова процедура, смартфон*.

Вступ. Практика показує, що кримінальні процесуальні інструменти та засоби отримання доказової інформації, зокрема приватної (персональної) інформації, що належить окремим громадянам, є досить ефективними та дієвими у процесі розслідування та розкриття злочинів, доказування винуватос-

ті та притягнення винних до кримінальної відповідальності[1]; але разом з тим, вони можуть становити серйозну небезпеку гарантіям захисту конституційних прав і свобод людини й громадянина в процесі здійснення кримінального провадження[2], особливо враховуючи невизначеність правового регулювання процесу отримання вказаного виду інформації, а також дефекти кримінального процесуального законодавства. Усе це, враховуючи стрімкі темпи розвитку телекомунікацій та всезагальної інформатизації практично всіх сфер суспільного життя, визначає **актуальність зазначеної тематики**. Саме тому постають актуальними та важливими питання застосування належної правової процедури у процесі притягнення до кримінальної відповідальності за тяжкі й особливо тяжкі злочинні діяння.

Мета й завдання дослідження. Не претендуючи на абсолютну вичерпність дослідження та вирішення означеної об'ємної проблематики, слід зазначити, що вона лежить не лише в площині кримінальних процесуальних правовідносин, але й зачіпає доволі широкий спектр відносин. Насамперед, це відносини у сферах адміністративного управління, конституційного, міжнародно-правового та цивільно-правового захисту особистих немайнових та

[1] Так, наприклад, як зазначають дослідники, лише шляхом проведення заходів негласного збирання інформації в кримінальних провадженнях або під час здійснення оперативно-розшукової діяльності, є можливим розслідування та розкриття більше 85 % тяжких та особливо тяжких злочинів. Див. детальніше: Погорецький М. А. Негласні слідчі (розшукові) дії: проблеми впровадження та використання результатів у доказуванні. *Юридичний часопис Національної академії внутрішніх справ України*. 2013. № 1. С. 270; Сергєєва Д. Використання результатів негласних слідчих (розшукових) дій для отримання окремих видів доказів у кримінальному провадженні: проблемні питання. *Право України*. 2017. № 12. С. 49; Шевчишен А. Можливості збирання доказів і розшуку при здійсненні окремих негласних слідчих (розшукових) дій у кримінальних провадженнях про корупційні злочини у сфері службової та професійної діяльності, пов'язаної з наданням публічних послуг. *Право України*. 2016. № 10. С. 178 та ін.

[2] Проблеми захисту права на повагу до приватного і сімейного життя, так звані «права на приватність» або «прайвесі» у найбільш широкому значенні, хоча і не є новими, але з кожним роком стають все більш актуальними та гострими в усьому світі, що пов'язане із постійним розвитком суспільних відносин, науково-технічним прогресом, глобалізацією та іншими факторами. Див. детальніше про цю проблематику, зокрема: Серьогін В. Зміст і обсяг права на недоторканність приватного життя (прайвесі). *Вісник Академії правових наук України*. 2010. № 4 (63). С. 88–97; Король І. Б. Охорона недоторканності приватного життя: кримінально-правові та кримінологічні аспекти: дис. … к.ю.н.: 12.00.08. Львів, 2015. 235 с.; Присяжнюк І. Недоторканність приватного життя як об'єкт кримінально-правової охорони. *Право України*. 2017. № 2. С. 131–138; Присяжнюк І. Дотримання права на приватність при здійсненні соціального контролю, спрямованого на протидію злочинності. *Право України*. 2017. № 12. С. 132–139; Панкевич О. Захист права на приватність: динаміка світоглядно-методологічних основ (за матеріалами практики Європейського суду з прав людини). *Право України*. 2017. № 4. С. 66–75; Каретник О. До питання про правову природу персональних даних фізичної особи: цивілістичні аспекти. *Право України*. 2014. № 9. С. 192–200 та ін.

майнових прав особи, здійснення підприємницької діяльності суб'єктів господарювання та надання медичних, інформаційних та інших послуг, надання послуг у сфері ІТ-технологій, обслуговування засобів телекомунікацій та багато інших, які тісно корелюють із відносинами щодо притягнення особи до кримінальної відповідальності. Однак, серед усього універсуму проблем, що виникають у цьому контексті, метою нашого дослідженні буде вивчення окремих проблемних аспектів належної правової процедури доступу до приватної інформації під час здійснення досудового розслідування злочинів; дослідження механізму правового регулювання формування відповідної доказової інформації; виявлення правової (законодавчої) невизначеності у зв'язку зі здійснення такої діяльності; а також висунення пропозицій щодо можливих шляхів вирішення вказаних проблем та неоднозначностей доктрини та правозастосовної практики.

Стан наукового дослідження проблематики. На сьогоднішній день комплексних досліджень вказаної проблематики небагато, до того ж висновки, отримані в результаті цих розробок, не завжди є однозначними, безспірними та вичерпними, враховуючи постійну безсистемну мінливість та недосконалість чинного законодавства, а також стрімкий розвиток інформаційних технологій, які непомітно, але досить впевнено стали невід'ємною частиною забезпечення користування й використання різних видів та форм інформації та людського спілкування у цілому. Тож, окремі аспекти окресленої проблематики, так чи інакше, були предметом вивчення, зокрема, таких вчених, як: Ю. Аленін, М. Багрій, С. Гриненко, О. Дроздов, О. Капліна, І. Король, С. Кудінов, Є. Лук'янчиков, В. Луцик, М. Погорецький, І. Присяжнюк, Д. Сергєєва, Л. Удалова, М. Цуцкірідзе, А. Шевчишен, В. Шепітько, Р. Шехавцов, О. Шило, Д. Шумейко, М. Шумило та ін.

Виклад основного матеріалу. На сьогодні у процесі здійснення кримінального провадження отримання доказової інформації, що становить персональні дані особи, а також відомостей стосовно обміну та використання

інформації, що може бути віднесено до приватного спілкування, у тому значенні, як його дає Кримінальний процесуальний кодекс України (далі – КПК), може здійснюватися різними способами. Найбільш ефективними, а відтак, і найбільш поширеними в практиці збирання доказів, є, зокрема: здійснення слідчих, негласних слідчих (розшукових) дій, а також окремих засобів забезпечення кримінального провадження (наприклад, тимчасовий доступ до речей і документів та тимчасове вилучення майна). Особливий інтерес, як убачається, викликають ті випадки, коли вказані процесуальні дії в кримінальному провадженні здійснюються у зв'язку із доступом до технічних засобів телекомунікації, персональних комп'ютерів, мобільних терміналів систем зв'язку, інших технічних пристроїв обробки та передавання інформації, ЕОМ. Зокрема тому більш детально в нашому дослідженні, вважаємо, слід зупинитися саме на цьому аспекті належної правової процедури отримання доказової інформації в кримінальному провадженні під час здійснення досудового розслідування.

Так, наприклад, найбільш частим і розповсюдженим способом спілкування між людьми є таке, що здійснюється за допомогою різноманітних технічних засобів (пристроїв) телекомунікації – мобільних (стільникових) телефонів, смартфонів, планшетних ПК, інших мобільних терміналів систем зв'язку, нетбуків, ноутбуків, персональних комп'ютерів тощо, у тому числі шляхом використання мережі Інтернет. Викликає неабиякий інтерес той факт, що за офіційними даними Реєстру радіоелектронних засобів та випромінювальних пристроїв, що можуть застосовуватися на території України в смугах радіочастот загального користування, станом на 1 листопада 2019 р. нараховується близько 20,7 тисяч конкретних типів радіоелектронних засобів та випромінювальних пристроїв[3]. І це лише ті, використання яких офіційно дозволено державою. За окремими підрахунками, на середину 2018 р. в світі нараховується

[3] Офіційний веб-портал Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=59&id=4182&language=uk (дата звернення: 17.05.2020).

близько 59 % користувачів смартфонів від усього дорослого населення планети[4]. В Україні за 2015–2016 рр. було продано більше 6 млн. штук смартфонів[5].

Актуальність та неоднозначність досліджуваної проблематики підсилює також і той факт, що в законодавстві та наукових джерелах відсутні єдині підходи до визначення понять і термінів, що позначають технічні засоби (пристрої) телекомунікації. Так, наприклад, в законодавстві зустрічаються такі терміни, як «пристрій», «радіоелектронний засіб», «засіб зв'язку», «мобільний термінал систем зв'язку», «інший радіовипромінювальний пристрій» та ін. Зокрема, відповідно до ст. 1 Закону України «Про радіочастотний ресурс України» від 1 червня 2000 р. № 1770-III, «радіоелектронний засіб – технічний засіб, призначений для передавання та/або приймання радіосигналів радіослужбами»[6].

Безумовно, що інформація, отримана внаслідок комунікації осіб, причетних до вчинення кримінальних правопорушень, може мати надзвичайно цінне значення для встановлення обставин, що стосуються події злочину, та може бути використана для розкриття злочинів та доказування вини осіб у їх вчиненні. Однак, як відомо, кримінальний процесуальний закон вимагає чіткого й неухильного дотримання нормативних конституційних і законодавчих приписів, а також забезпечення гарантій прав і свобод людини й громадянина під час кримінального провадження, з тим, щоб отримані докази були допустимими й могли бути використані в процесі доказування. Саме тому необхідно проаналізувати окремі особливості належної правової процедури збирання й перевірки вказаної доказової інформації, що може бути отримана із вказаних «ґаджетів». До сказаного не зайвим буде також додати, що з практики

[4] Poushter Jacob, Bishop Caldwell, Chwe Hanyu. Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones. Digital divides remain, both within and across countries. URL: http://www.pewglobal.org/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/ (дата звернення: 20.05.2020).

[5] Смартфон. Вікіпедія: веб-сайт. URL: https://uk.m.wikipedia.org/wiki/Смартфон (дата звернення: 17.05.2020).

[6] Про радіочастотний ресурс України: Закон України від 1 червня 2000 р. № 1770-III. Дата оновлення: 13 лютого 2020 р. URL: http://zakon.rada.gov.ua/laws/show/1770-14 (дата звернення: 17.05.2020).

Європейського Суду з прав людини (далі – ЄСПЛ) випливає також і те, що втручання органів державної влади можливе не лише тоді, коли воно здійснюється «згідно із законом», але й коли воно має «законну мету» та є «пропорційним»[7].

Системний аналіз чинного кримінального процесуального законодавства дає підстави стверджувати, що на сьогодні відсутній єдиний уніфікований процесуальний механізм (алгоритм) отримання доступу до (збирання в широкому значенні) інформації, що міститься, або яку можливо отримати за допомогою указаних технічних засобів телекомунікації. Більше того, правозастосовна практика також виробила різні й не завжди правильні шляхи вирішення вказаного питання. Так, наприклад, на сьогодні досить поширеною є практика виявлення, фіксації та використання інформації, що міститься в мобільних телефонах чи смартфонах, шляхом проведення огляду останніх. В інших випадках можуть бути проведені такі негласні слідчі (розшукові) дії (далі – НСРД), як зняття інформації з транспортних телекомунікаційних мереж (далі – ЗІТТМ) або зняття інформації з електронних інформаційних систем (далі – ЗІЕІС).

Як убачається, така неоднозначність зумовлена невизначеністю правового регулювання вказаного питання, а також самою специфікою, неоднаковою технічною та правовою природою зазначених вище технічних засобів (пристроїв) телекомунікації та інформації, що зберігається, обробляється та використовується за допомогою останніх. Так, наприклад, мобільний термінал систем зв'язку – «смартфон» – може бути використаний як:

1) засіб для спілкування в реальному часі («он-лайн»), наприклад, для здійснення телефонних дзвінків;

2) засіб доступу до електронних інформаційних систем шляхом використання різних форм передавання даних, у тому числі, як правило, через ме-

[7] Див., зокрема, рішення ЄСПЛ у справі «Бенедік проти Словенії» від 24 квітня .2018 р. (Справа «Бенедикт проти Словенії» (повний текст рішення). URL: https://www.echr.com.ua/translation/sprava-benedik-proti-slovenii-povnij-tekst-rishennya/ (дата звернення: 17.05.2020)).

режу Інтернет (наприклад, для спілкування в різноманітних чатах, соцмережах, зокрема, Facebook, Twitter, Instagram, Telegram, Snapchat etc; або для використання електронної пошти, у тому числі з використанням так званих «хмарних технологій» («хмарних обчислень») зберігання й обробки інформації (до прикладу Google Drive чи подібних); або з використанням так званих «месенджерів», наприклад, Viber, WhatsApp, Skype, Facebook Messenger, Telegram etc). Як зазначають дослідники, вказані телекомунікаційні технології являють собою конвергенцію мереж, які підтримують широкий спектр методів доступу (традиційна телефонія, DSL, мережі WLAN, RAN та ін.); на рівні конвергенції послуг під час сесій зв'язку мобільного терміналу за допомогою спеціалізованого програмного забезпечення може здійснюватися мобільний доступ до даних, проведення аудіо- та відеоконфренцій, передача голосу та миттєвий обмін повідомленнями. Широке використання абонентами рухомого (мобільного) зв'язку смартфонів зі встановленими на них програмами, які суміщають у собі сервіси IP-телефонії та месенджерів (Skype, Viber та ін.) або тільки месенджерів (ICQ, Telegram, WhatsApp та ін.), утворюють із них елементи розподілених електронних інформаційних систем (РІС)[8]. Компоненти РІС розподілені, отже, по декількох комп'ютерах. У свою чергу, РІС поділяються на файл-серверні інформаційні системи та клієнт-серверні інформаційні системи. В останніх, до прикладу, база даних та система управління базою даних знаходяться на сервері, а на робочих станціях знаходиться клієнтське програмне забезпечення[9]. При цьому слід вказати на одну досить істотну особливість. Інформація, яка відображається на екрані пристрою, як правило, фізично на ньому не зберігається; вона зберігається в електронних ін-

[8] Цит. за: Шевчишен А. Можливості збирання доказів і розшуку при здійсненні окремих негласних слідчих (розшукових) дій у кримінальних провадженнях про корупційні злочини у сфері службової та професійної діяльності, пов'язаної з наданням публічних послуг. С. 180.

[9] Як зазначається в літературі, як локальні, так і розподілені електронні інформаційні системи, можуть бути відкритими для громадян, так і закритими, тобто доступ до яких обмежений їх власником, володільцем або утримувачем. Більш детально про особливості окремих електронних інформаційних систем та ЗІЕІС. Див.: Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: навчально-практичний посібник. Харків: Оберіг, 2013. С. 43.

формаційних системах (інформаційних (автоматизованих) системах), на серверах відповідних компаній[10], які забезпечують надання відповідних інформаційно-телекомунікаційних послуг. Тобто в цьому разі мобільний пристрій слугує лише засобом доступу (таким собі «ключем») до інформації, що становить зміст спілкування. В іншому ж разі, якщо вказана інформація зберігається в пам'яті самого пристрою, особливості використання останнього будуть описані нижче, в третій групі. Окрім цього, необхідно також зробити зауваження відносно того, що деякі із вказаних месенджерів чи соцмереж дозволяють також здійснювати спілкування в реальному часі («он-лайн»); тому за таких випадків смартфон за своїм функціональним (функціонально-технічним та комунікаційним) призначенням слід віднести до попередньої групи;

3) засіб зберігання та/або обробки даних (найрізноманітніших текстових, графічних, аудіо-, відео- та інших файлів і медіаданих). Так, наприклад, у пам'яті пристрою можуть зберігатися надіслані й збережені користувачем аудіо-, відео-, фотофайли, СМС-повідомлення тощо. Доступ до цієї інформації на технічному пристрої може здійснюватися як за допомогою безпосередньо операційної системи останнього, так і за допомогою спеціально встановленого програмного забезпечення, так званих прикладних програм, «застосунків» (широко відомого користувачам як «мобільний додаток» або просто «додаток»).

Як убачається, отже, зважаючи на різне функціональне призначення вказаних мобільних терміналів систем зв'язку, отримання доступу до інформації, що на них міститься, має здійснюватися диференційовано, у різному процесуальному порядку, з використанням різних способів збирання доказо-

[10] Винятком може слугувати, до прикладу, Viber та деякі інші, інформація про зміст повідомлень, надіслані файли тощо з яких фізично міститься (зберігається) у пам'яті самого технічного пристрою, оскільки, як заявляє сама компанія, інформація про зміст повідомлень видаляється із серверів компанії відразу після того, як повідомлення буде надіслано кінцевому користувачеві. Див. детальніше з цього приводу про політику конфіденційності та безпеки спілкування у Viber: The most secure messaging app. URL: https://www.viber.com/security (дата звернення: 23.05.2020).

вої інформації, з урахуванням у кожному конкретному випадку вищенаведених особливостей. Таким чином, належна правова процедура процесуального порядку, способів отримання доказової інформації у контексті доступу до неї з використанням названих мобільних терміналів систем зв'язку (технічних засобів телекомунікації), має здійснюватися в такому порядку.

А. У першому випадку, коли мобільний пристрій використовується як засіб для спілкування в реальному часі («он-лайн»), інформація, що становить зміст приватного спілкування, може бути отримана шляхом проведення такої НСРД, як ЗІТТМ, оскільки передавання даних здійснюється шляхом використання відповідних технічних можливостей транспортних телекомунікаційних мереж (каналів зв'язку)[11]. Слід враховувати, що коли спілкування відбувається в режимі реального часу за допомогою (посередництвом) програмного забезпечення пристрою, що здійснює передачу даних через соцмережі або подібні он-лайн сервіси, тобто забезпечує зв'язок із електронними інформаційними системами (інформаційними (автоматизованими) системами), що знаходяться на серверах відповідних компаній, то отримання доступу до такої інформації саме у зв'язку з «проникненням» в зазначені системи необхідно здійснювати шляхом проведення такої НСРД, як ЗІЕІС.

Б. У другому випадку, коли смартфон (чи інший технічний пристрій) слугує лише засобом доступу до інформації, що зберігається в електронних інформаційних системах, та лише відображається на екрані пристрою, але фізично не зберігається на ньому, отримати та зафіксувати (скопіювати) таку інформацію необхідно шляхом проведення такої НСРД, як ЗІЕІС[12]. А тому вважаємо, що інакша практика у цих випадках, наприклад, отримання інфор-

[11] Більш детально про специфіку здійснення ЗІТТМ та особливості окремих типів транспортних телекомунікаційних мереж (каналів зв'язку) див.: Багрій М., Луцик В. Деякі проблеми законодавчого регулювання проведення негласних слідчих (розшукових) дій. *Право України*. 2017. № 12. С. 45; Сергєєва Д. Проблемні аспекти використання результатів зняття інформації з транспортних телекомунікаційних мереж як доказів у кримінальному провадженні. *Право України*. 2014. № 11. С. 209–218 та ін.

[12] Така інформація в суді визнається як належний і допустимий доказ, що знаходить своє підтвердження в судовій практиці. Див., з-поміж інших, наприклад: Вирок Шевченківського районного суду м. Чернівці від 17 травня 2018 р., судове провадження № 1-кп/727/186/18. URL: http://reyestr.court.gov.ua/Review/74052875 (дата звернення: 23.05.2020).

мації шляхом здійснення звичайного огляду технічного пристрою, тобто як слідчої дії («гласної»), є незаконною та неправомірною[13]. Саме тому цілком погоджуємося із тими судами, які визнають внаслідок цього такі докази недопустимими[14].

Складність телекомунікаційних технологій, зокрема тих, що застосовують сервіси PIC, а також невизначеність правового регулювання у зв'язку із цим, породжують також й інші неоднозначні випадки на практиці. Так, А. Шевчишен описує такі приклади. Не маючи точних даних, у який спосіб буде здійснене спілкування особи абонента оператора рухомого (мобільного) зв'язку (звичайної голосової телефонії, IP-телефонії або месенджерів), слідчі одночасно отримують дозволи на проведення ЗІТТМ і ЗІЕІС. Уповноважені оперативні підрозділи, які виконують доручення на проведення цих НСРД відносно абонента оператора рухомого (мобільного) зв'язку, по суті одночасно проводять ці дві процесуальні дії та в підсумку складають один протокол (про ЗІТТМ або ЗІЕІС), що в суді визнається джерелом доказів[15]. Не заперечуючи вцілому можливість отримання слідчим дозволів на проведення декількох НСРД, зокрема, ЗІТТМ та ЗІЕІС (оскільки процесуальний порядок здійснення судового контролю та інші гарантії забезпечення захисту прав особи під час проведення таких форм втручання в приватне спілкування є однаковим, не беручи до уваги виняток, передбачений ч. 2 ст. 264 КПК, про що буде згадано нижче; а також тому що дійсно не можливо з точністю знати

[13] І, на жаль, суди досить часто визнають такі матеріали допустимими доказами. Див., наприклад: Вирок Васильківського міськрайонного суду Київської області від 4 грудня 2015 р., судове провадження № 1-кп/362/117/15. URL: http://reyestr.court.gov.ua/Review/54439563 (дата звернення: 23.05.2020); Вирок Автозаводського районного суду м. Кременчука Полтавської області від 13 серпня 2018 р., судове провадження № 1-кп/524/90/18. URL: http://reyestr.court.gov.ua/Review/75827069 (дата звернення: 23.05.2020); Вирок Подільського районного суду м. Києва від 7 листопада 2016 р., судове провадження № 1-кп/758/378/16. URL: http://reyestr.court.gov.ua/Review/62532485 (дата звернення: 24.05.2020) та ін.

[14] Див.: Вирок Орджонікідзевського районного суду м. Маріуполя Донецької області від 12 квітня 2017 р., судове провадження № 1-кп/265/46/17. URL: http://reyestr.court.gov.ua/Review/65990469 (дата звернення: 24.05.2020); Вирок Личаківського районного суду м. Львова від 6 лютого 2017 р., судове провадження № 1-кп/463/40/17. URL: http://reyestr.court.gov.ua/Review/64527701 (дата звернення: 23.05.2020) та ін.

[15] Шевчишен А. Можливості збирання доказів і розшуку при здійсненні окремих негласних слідчих (розшукових) дій у кримінальних провадженнях про корупційні злочини у сфері службової та професійної діяльності, пов'язаної з наданням публічних послуг. С. 180–181.

наперед, враховуючи вищенаведені особливості використання сучасних телекомунікаційних технологій, які саме технічні можливості свого «ґаджету» застосує особа в процесі спілкування), загалом погоджуємося з думкою автора про те, що результати цих дій слід фіксувати в окремих протоколах. А також, щоб уникнути в майбутньому спірних практичних ситуацій, цілком підтримуємо пропозицію А. Шевчишена щодо «необхідності проведення предметного дослідження доцільності окремого існування НСРД, передбачених статтями 263 та 264 КПК України»[16], з тим, щоб збирання цінної доказової інформації було здійснене в рамках належної правової процедури в кримінальному провадженні[17].

При цьому на практиці може виникнути питання щодо застосування ч. 2 ст. 264 КПК стосовно здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, з використанням вилученого технічного пристрою, без дозволу слідчого судді. Вважаємо, що навіть у цьому випадку, якщо слідчий (співробітник оперативного підрозділу), які мають намір отримати інформацію із застосуванням вилученого технічного пристрою, необхідно отримувати дозвіл слідчого судді на проведення цієї НСРД. Це пояснюється тим, що технічний пристрій завжди є таким собі «персональним ключем» доступу до особистої інформації конкретного користувача, є його власністю, та здатен забезпечити не лише ознайомлення із змістом інформації, як це можуть вільно зробити й інші користувачі конкретної соцмережі або подібного он-лайн сервісу, але і здатен забезпечити керування та обробку цієї інформації (тобто можливість

[16] Шевчишен А. Можливості збирання доказів і розшуку при здійсненні окремих негласних слідчих (розшукових) дій у кримінальних провадженнях про корупційні злочини у сфері службової та професійної діяльності, пов'язаної з наданням публічних послуг. С. 181.

[17] Або ж навпаки, можливо більш доцільно було б, враховуючи специфіку застосувння РІС, передбачити на рівні закону можливість проведення окремої НСРД, пов'язаної із втручанням у приватне спілкування, з використанням доступу через радіоелектронний технічний засіб (мобільний термінал систем зв'язку). Без претензій на істинність цієї пропозиції, відмітимо, що вона має стати предметом обговорення фахівців як інформаційно-технічної сфери, так і працівників судових та правоохоронних органів, із залученням правників-науковців.

внесення змін, доповнень до неї, її видалення, переміщення на інші носії тощо). У разі ж, якщо суб'єкт, що здійснюватиме ЗІЕІС, з метою пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частині, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, без використання вилученого технічного пристрою (у тому числі якщо він не буде використаний як засіб пошуку чи виявлення інформації, що цікавить слідчого), а в інший спосіб, шляхом використання певних пристроїв, які жодним чином не пов'язані із вилученим «ґаджетом» особи, то думається, що в такому разі немає підстав для незастосування ч. 2 ст. 264 КПК, і отже, відсутня необхідність для отримання дозволу слідчого судді на проведення ЗІЕІС.

При цьому і в першому, і в другому випадках необхідно пам'ятати, що згідно ч. 5 ст. 258 КПК, у будь-якому разі, втручання у приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим заборонене.

В. Нарешті, у третьому випадку, коли, по-суті, пристрій є технічним носієм інформації, що зберігається на ньому, останній має всі ознаки, які притаманні речовим доказам або документам (у даному разі – це є електронні документи) у кримінальному провадженні. А тому лише в цьому разі доступ до даних, що містяться на технічному пристрої (мобільному терміналі систем зв'язку), та які отримані та збережені користувачем (чи автоматично збережені на цьому пристрої), і користувач ознайомлений з їхнім змістом, може бути отримано таким же процесуальним шляхом, як і будь-які інші речі або документи в кримінальному провадженні. Тобто, зокрема, вилучення мобільного пристрою та ознайомлення із змістом інформації на ньому може здійснюватися у зв'язку з проведенням обшуку, огляду житла чи іншого володіння особи, обшуку особи під час проведення обшуку в житлі чи іншому володінні, тимчасового вилучення майна під час законного затримання особи в порядку статей 207, 208 КПК, проведенням тимчасового доступу до речей і документів та ін.

Ознайомлення із змістом відомостей, що містяться (зберігаються) на вилученому в такий спосіб пристрої, копіювання відповідних електронних документів необхідно здійснювати під час огляду цього пристрою, у тому числі із використанням допомоги спеціаліста (у разі виникнення необхідності застосувати спеціальні знання фахівців-експертів при дослідженні пристрою або інформації, що міститься на ньому, можливе також залучення експерта та проведення експертизи в порядку, визначеному процесуальним законом)[18]. При цьому необхідно пам'ятати деякі вимоги кримінального процесуального закону в разі доступу до технічних засобів телекомунікації, зокрема:

по-перше, вимоги абз. 2 ч. 1 ст. 159, п. 7 ч. 2 ст. 160, ч. 7 ст. 163, ч. 2 ст. 168 КПК щодо можливості вилучення відповідних пристроїв під час тимчасового доступу до речей і документів, вилучення майна під час обшуку, огляду, законного затримання особи;

по-друге, вимоги ст. 161 КПК щодо заборони за будь-яких умов під час провадження тимчасового доступу до речей і документів отримувати доступ до тих речей і документів, у яких міститься інформація, що становить адвокатську таємницю;

по-третє, вимоги п.п. 6, 7 ч. 2 ст. 160, ст. 162, ч. 6 ст. 163 КПК під час здійснення тимчасового доступу до речей і документів щодо можливості отримання доступу до інформації, що містить охоронювану законом таємницю. Слід зазначити, що практично завжди така інформація міститься на відповідних технічних пристроях, оскільки, відповідно до ст. 162 КПК, до охоронюваної законом таємниці, яка міститься в речах і документах, належать, зокрема: конфіденційна інформація, особисте листування особи та інші записи особистого характеру, інформація про зв'язок, абонента, надання телеко-

[18] Такий підхід підтверджується і в численних судових рішеннях. Див., наприклад: Вирок Слов'янського міськрайонного суду Донецької області від 19 листопада 2015 р., судове провадження № 1-кп/243/517/2015. URL: http://reyestr.court.gov.ua/Review/53596315 (дата звернення: 23.05.2020); Вирок Золотоніського міськрайонного суду Черкаської області від 23 вересня 2015 р., судова справа № 695/1637/15-к. URL: http://reyestr.court.gov.ua/Review/51808318 (дата звернення: 23.05.2020); Вирок Вишгородського районного суду Київської області від 17 травня 2013 р., судова справа № 1-КП-4/2013. URL: http://reyestr.court.gov.ua/ Review/31379448 (дата звернення: 23.05.2020) та ін.

мунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних. Ще більш широкого змісту така інформація набуває у контексті правової позиції Конституційного Суду України, сформованої в його рішенні від 20 січня 2012 р., № 2-рп/2012: «перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним; належність інформації про фізичну особу до конфіденційної визначається в кожному конкретному випадку» (п. п. 3.2–3.3 мотивувальної частини рішення); у будь-якому разі, інформація про особисте та сімейне життя особи є конфіденційною інформацією (п. 1 резолютивної частини рішення)[19]. Така позиція повністю узгоджується із практикою, сформованою ЄСПЛ, який зазначає, що: «“приватне життя” є дуже широким поняттям, яке не має вичерпного визначення» (п. 57 рішення по справі «Пек v. Сполученого Королівства»; п. 95 рішення по справі «Смірнови v. Російської Федерації»), і тому ЄСПЛ «не вважає за можливе і необхідне дати вичерпне визначення поняттю “приватне життя”» (п. 29 рішення по справі «Німітц v. Німеччини»)[20]. Більше, привертає увагу той факт, що в одному із нещодавніх своїх рішень ЄСПЛ до елементів приватного життя відніс також інформацію про IP-адресу, що належить користувачу; а ідентифікація користувача Інтернету за IP-адресою є, відповідно, втручанням у його право на повагу до приватного життя (рішення у справі «Бенедік v. Словенії» від 24 квітня 2018 р.)[21].

Задля справедливості дослідження зауважимо, що навіть у цьому разі, під час вилучення та огляду мобільного пристрою, можна буде ознайомитися

[19] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: http://zakon4.rada.gov.ua/laws/show/v002p710-12/print1389947652746863 (дата звернення: 26.05.2020).

[20] Цит. за: Панкевич О. Захист права на приватність: динаміка світоглядно-методологічних основ (за матеріалами практики Європейського суду з прав людини). С. 67.

[21] ЄСПЛ визнав, що IP-адреса є елементом приватного життя. Рішення у справі «Бенедік проти Словенії». URL: https://www.echr.com.ua/yespl-viznav-shho-ip-adresa-ye-elementom-privatnogo-zhittya/ (дата звернення: 26.05.2020).

з інформацією, яка фізично зберігається на ньому, та яка становить зміст тої, що може бути віднесена до приватного спілкування (в розумінні кримінального процесуального закону), наприклад, отримані та збережені на пристрої СМС-повідомлення, з якими особа вже ознайомилася. Однак для отримання цієї інформації відсутня необхідність проведення НСРД, що пов'язані із втручанням у приватне спілкування. Для підтвердження цієї позиції можна як приклад навести таку аналогію. «Класичні» паперові листи, що надсилаються з використанням поштового зв'язку, а так само бандеролі, посилки тощо, в розумінні, що надається в ст. 1 Закону України «Про поштовий зв'язок» від 4 жовтня 2011 р. № 2759-III [22], які отримані особою (адресатом, одержувачем) та зберігаються нею як речі чи документи в житлі чи іншому володінні, також не потребують проведення НСРД для отримання доступу до таких речей чи документів або їх вилучення (вони можуть бути отримані, наприклад, шляхом проведення обшуку). Подібна ситуація виникає і з електронними документами, які так само зберігаються в особи, але вже з використанням технічних засобів (пристроїв) оброки електронної (цифрової) інформації.

До вищесказаного слід особливо також додати ще таку, як думається, досить важливу тезу. Нерідко на практиці можуть виникнути такі обставини, коли після вилучення та дослідження слідчим (за участі спеціаліста або без такого[23]) технічного пристрою (мобільний телефон, смартфон), його огляду, виявлення, копіювання та фіксації інформації, що міститься на ньому, на цей пристрій може в подальшому також надходити нова інформація, нові повідомлення, в режимі «реального часу», про що особі, якій належить цей «ґаджет», буде невідомо. За таких умов, вважаємо, ці нові повідомлення підпадають під інформацію в контексті приватного спілкування, оскільки вони ще

[22] Про поштовий зв'язок: Закон України від 4 жовтня 2011 р. № 2759-III. Дата оновлення: 13 лютого 2020 р. URL: http://zakon.rada.gov.ua/laws/show/2759-14 (дата звернення: 26.05.2020).

[23] Необхідно при цьому враховувати, що під час здійснення тимчасового вилучення майна, відповідно до абз. 4 ч. 2 ст. 168 КПК, у разі необхідності слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

не дійшли до свого кінцевого отримувача (адресата) та не були доведені до його відома (тобто не були ознайомлені ним із змістом такої інформації). А тому в цих випадках, переконані, найбільш правильними, що будуть відповідати критеріям належної правової процедури та принципам верховенства права, законності, таємниці спілкування, невтручання у приватне життя, забезпечення права на захист, способами доступу до вказаної інформації будуть такі, що застосовуються у зв'язку із втручанням у приватне спілкування, тобто шляхом проведення таких НСРД, як ЗІТТМ або ЗІЕІС, залежно від виду та способу надходження такої інформації та функціонального призначення технічного пристрою, про що було зазначено вище. Наприклад, у разі надходження СМС-повідомлення – здійснити ЗІТТМ; у разі надходження повідомлення в соцмережі, до прикладу, Facebook, – здійснити ЗІЕІС. З цією метою може бути рекомендовано слідчому, прокурору звернутися у визначеному законом порядку до слідчого судді апеляційного суду для отримання дозволу на проведення вказаних НСРД, не чекаючи, поки на вилучений технічний пристрій надійде нова інформація. Саме в такому разі, вважаємо, буде забезпечено законність (допустимість) отримання доказової інформації та можливість у подальшому її використання в суді.

Результати дослідження. Враховуючи різне функціональне призначення технічних засобів телекомунікації, отримання доступу та збирання доказової інформації, що на них міститься, повинно здійснюватися диференційовано, у різній процесуальній формі (формування доказової інформації можливе як шляхом здійснення «традиційних» слідчих дій, так і окремих НСРД чи заходів забезпечення кримінального провадження), з урахуванням, безумовно, у кожному конкретному випадку специфіки телекомунікаційних технологій, що було проілюстровано вище; а також з урахуванням підстав, умов та конкретних процедурних і тактичних особливостей здійснення кожної конкретної процесуальної дії.

При характеристиці процесуального порядку отримання (збирання) доказової інформації в нашій роботі як приклад використано було смартфон як мобільний термінал систем зв'язку (технічний засіб зв'язку, пристрій телекомунікації). Однак за тим же принципом, враховуючи подібність технічної та правової природи, подібність алгоритмів збирання, зберігання, обробки, передачі та використання інформації, функціональне призначення тощо, вказані способи процесуального порядку доступу до (збирання) доказової інформації можливо застосовувати й до інших видів технічних засобів (пристроїв) телекомунікації (персональних комп'ютерів, планшетних ПК, ноутбуків та ін.).

Висновки. Підсумовуючи все вищесказане, можна резюмувати, що окремі форми процесуальних механізмів забезпечення невідворотності кримінальної відповідальності потребують якнайшвидшого реформування та уніфікації задля забезпечення алгоритмізації, одноманітності та сталості правозастосовної практики. Усе це неможливе без того, щоб збирання цінної доказової інформації в кримінальному провадженні було здійснене в рамках належної правової процедури й із дотриманням прав людини й основоположних свобод під час здійснення досудового розслідування злочинів.

Список використаних джерел

1. The most secure messaging app. URL: https://www.viber.com/security (дата звернення: 23.05.2020).

2. Багрій М., Луцик В. Деякі проблеми законодавчого регулювання проведення негласних слідчих (розшукових) дій. *Право України*. 2017. № 12. С. 39–48.

3. Вирок Автозаводського районного суду м. Кременчука Полтавської області від 13 серпня 2018 р., судове провадження № 1-кп/524/90/18. URL: http://reyestr.court.gov.ua/Review/75827069 (дата звернення: 23.05.2020).

4. Вирок Васильківського міськрайонного суду Київської області від 4 грудня 2015 р., судове провадження № 1-кп/362/117/15. URL: http://reyestr.court.gov.ua/Review/54439563 (дата звернення: 23.05.2020).

5. Вирок Вишгородського районного суду Київської області від 17 трравня 2013 р., судова справа № 1-КП-4/2013. URL: http://reyestr.court.gov.ua/ Review/31379448 (дата звернення: 23.05.2020).

6. Вирок Золотоніського міськрайонного суду Черкаської області від 23 вересня 2015 р., судова справа № 695/1637/15-к. URL: http://reyestr.court.gov. ua/Review/51808318 (дата звернення: 23.05.2020).

7. Вирок Личаківського районного суду м. Львова від 6 лютого 2017 р., судове провадження № 1-кп/463/40/17. URL: http://reyestr.court.gov.ua/ Review/64527701 (дата звернення: 23.05.2020).

8. Вирок Орджонікідзевського районного суду м. Маріуполя Донецької області від 12 квітня 2017 р., судове провадження № 1-кп/265/46/17. URL: http://reyestr.court.gov.ua/Review/65990469 (дата звернення: 24.05.2020).

9. Вирок Подільського районного суду м. Києва від 7 листопада 2016 р., судове провадження № 1-кп/758/378/16. URL: http://reyestr.court.gov.ua/Review/62532485 (дата звернення: 24.05.2020).

10. Вирок Слов'янського міськрайонного суду Донецької області від 19 листопада 2015 р., судове провадження № 1-кп/243/517/2015. URL: http://reyestr.court.gov.ua/Review/53596315.

11. Вирок Шевченківського районного суду м. Чернівці від 17 травня 2018 р., судове провадження № 1-кп/727/186/18. URL: http://reyestr.court.gov.ua/Review/74052875 (дата звернення: 23.05.2020).

12. Дослідження, проведене аналітичною компанією Pew Research Center. URL: http://www.pewglobal.org/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/pg_2018-06-19_global-tech_2-00/ (дата звернення: 20.05.2020).

13. ЄСПЛ визнав, що IP-адреса є елементом приватного життя. Рішення у справі «Бенедік проти Словенії». URL: https://www.echr.com.ua/yespl-viznav-shho-ip-adresa-ye-elementom-privatnogo-zhittya/ (дата звернення: 26.05.2020).

14. Каретник О. До питання про правову природу персональних даних фізичної особи: цивілістичні аспекти. *Право України*. 2014. № 9. С. 192–200.

15. Король І. Б. Охорона недоторканності приватного життя: кримінально-правові та кримінологічні аспекти: дис. … к.ю.н.: 12.00.08. Львів, 2015. 235 с.

16. Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: навчально-практичний посібник. Харків: Оберіг, 2013. 344 с.

17. Офіційний веб-портал Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації. URL: https://nkrzi.gov.ua/ index.php?r=site/index&pg=59&id=4182&language=uk (дата звернення: 17.05.2020).

18. Панкевич О. Захист права на приватність: динаміка світоглядно-методологічних основ (за матеріалами практики Європейського суду з прав людини). *Право України*. 2017. № 4. С. 66–75.

19. Погорецький М. А. Негласні слідчі (розшукові) дії: проблеми впровадження та використання результатів у доказуванні. *Юридичний часопис Національної академії внутрішніх справ України*. 2013. № 1. С. 270–276.

20. Присяжнюк І. Дотримання права на приватність при здійсненні соціального контролю, спрямованого на протидію злочинності. *Право України*. 2017. № 12. С. 132–139.

21. Присяжнюк І. Недоторканність приватного життя як об’єкт кримінально-правової охорони. *Право України*. 2017. № 2. С. 131–138.

22. Про поштовий зв'язок: Закон України від 4 жовтня 2011 р. № 2759-III. Дата оновлення: 13 лютого 2020 р. URL: http://zakon.rada.gov.ua/laws/show/2759-14 (дата звернення: 26.05.2020).

23. Про радіочастотний ресурс України: Закон України від 1 червня 2000 р. № 1770-III. Дата оновлення: 13 лютого 2020 р. URL: http://zakon.rada.gov.ua/laws/show/1770-14 (дата звернення: 17.05.2020).

24. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: http://zakon4.rada.gov.ua/laws/show/v002p710-12/print1389947652746863 (дата звернення: 26.05.2020).

25. Сергєєва Д. Проблемні аспекти використання результатів зняття інформації з транспортних телекомунікаційних мереж як доказів у кримінальному провадженні. *Право України*. 2014. № 11. С. 209–218.

26. Сергєєва Д. Використання результатів негласних слідчих (розшукових) дій для отримання окремих видів доказів у кримінальному провадженні: проблемні питання. *Право України*. 2017. № 12. С. 49–61.

27. Серьогін В. Зміст і обсяг права на недоторканність приватного життя (прайвесі). *Вісник Академії правових наук України*. 2010. № 4 (63). С. 88–97.

28. Смартфон. Вікіпедія: веб-сайт. URL: https://uk.m.wikipedia.org/wiki/Смартфон (дата звернення: 17.05.2020).

29. Справа «Бенедикт проти Словенії» (повний текст рішення). URL: https://www.echr.com.ua/translation/sprava-benedik-proti-slovenii-povnij-tekst-rishennya/ (дата звернення: 17.05.2020).

30. Шевчишен А. Можливості збирання доказів і розшуку при здійсненні окремих негласних слідчих (розшукових) дій у кримінальних провадженнях про корупційні злочини у сфері службової та професійної діяльності, пов'язаної з наданням публічних послуг. *Право України*. 2016. № 10. С. 177–185.

REFERENCES

1. Poushter, Jacob, Bishop, Caldwell, Chwe, Hanyu. (2018). Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones. Digital divides remain, both within and across countries URL: http://www.pewglobal.org/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/.

2. The most secure messaging app. (2020). URL: https://www.viber.com/security.

3. Bahriy, M., Lutsyk, V. (2017). Deyaki problemy zakonodavchoho rehulyuvannya provedennya nehlasnykh slidchykh (rozshukovykh) diy. *Pravo Ukrayiny – Law of Ukraine, 12, 39–48* [in Ukrainian].

4. Vyrok Avtozavods′koho rayonnoho sudu m. Kremenchuka Poltavs′koyi oblasti vid 13 serpnya 2018 r., sudove provadzhennya № 1-kp/524/90/18. (2018). URL: http://reyestr.court.gov.ua/Review/75827069 [in Ukrainian].

5. Vyrok Vasyl′kivs′koho mis′krayonnoho sudu Kyyivs′koyi oblasti vid 4 hrudnya 2015 r., sudove provadzhennya № 1-kp/362/117/15. (2015). URL: http://reyestr.court.gov.ua/Review/54439563 [in Ukrainian].

6. Vyrok Vyshhorods′koho rayonnoho sudu Kyyivs′koyi oblasti vid 17 trravnya 2013 r., sudova sprava № 1-KP-4/2013. (2013). URL: http://reyestr.court.gov.ua/Review/31379448 [in Ukrainian].

7. Vyrok Zolotonis′koho mis′krayonnoho sudu Cherkas′koyi oblasti vid 23 veresnya 2015 r., sudova sprava № 695/1637/15-k. (2015). URL: http://reyestr.court.gov.ua/Review/51808318 [in Ukrainian].

8. Vyrok Lychakivs′koho rayonnoho sudu m. L′vova vid 6 lyutoho 2017 r., sudove provadzhennya № 1-kp/463/40/17. (2017). URL: http://reyestr.court.gov.ua/Review/64527701 [in Ukrainian].

9. Vyrok Ordzhonikidzevs′koho rayonnoho sudu m. Mariupolya Donets′koyi oblasti vid 12 kvitnya 2017 r., sudove provadzhennya № 1-kp/265/46/17. (2017). URL: http://reyestr.court.gov.ua/Review/65990469 [in Ukrainian].

10. Vyrok Podil′s′koho rayonnoho sudu m. Kyyeva vid 7 lystopada 2016 r., sudove provadzhennya № 1-kp/758/378/16. (2016). URL: http://reyestr.court.gov.ua/Review/62532485 [in Ukrainian].

11. Vyrok Slov″yans′koho mis′krayonnoho sudu Donets′koyi oblasti vid 19 lystopada 2015 r., sudove provadzhennya № 1-kp/243/517/2015. (2015). URL: http://reyestr.court.gov.ua/Review/53596315 [in Ukrainian].

12. Vyrok Shevchenkivs′koho rayonnoho sudu m. Chernivtsi vid 17 travnya 2018 r., sudove provadzhennya № 1-kp/727/186/18. (2018). URL: http://reyestr.court.gov.ua/ Review/74052875 [in Ukrainian].

13. YeSPL vyznav, shcho IP-adresa ye elementom pryvatnoho zhyttya. Rishennya u spravi «Benedik proty Sloveniyi». (2018). URL: https://www.echr.com.ua/ yespl-viznav-shho-ip-adresa-ye-elementom-privatnogo-zhittya/ [in Ukrainian].

14. Karetnyk, O. (2014). Do pytannya pro pravovu pryrodu personal′nykh danykh fizychnoyi osoby: tsyvilistychni aspekty. *Pravo Ukrayiny – Law of Ukraine, 9, 192–200* [in Ukrainian].

15. Korol′, I.B. (2015). Okhorona nedotorkannosti pryvatnoho zhyttya: kryminal′no-pravovi ta kryminolohichni aspekty. *Candidate's thesis*. L′viv [in Ukrainian].

16. Kudinov, S.S., Shekhavtsov, R.M., Drozdov, O.M., Hrynenko, S.O. (2013). Nehlasni slidchi (rozshukovi) diyi ta vykorystannya rezul′tativ operatyvno-rozshukovoyi diyal′nosti u kryminal′nomu provadzhenni. Kharkiv: Oberih [in Ukrainian].

17. Ofitsiynyy veb-portal Natsional′noyi komisiyi, shcho zdiysnyuye derzhavne rehulyuvannya u sferi zv″yazku ta informatyzatsiyi. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=59&id=4182&language=uk [in Ukrainian].

18. Pankevych, O. (2017). Zakhyst prava na pryvatnist′: dynamika svitohlyadno-metodolohichnykh osnov (za materialamy praktyky Yevropeys′koho sudu z prav lyudyny). *Pravo Ukrayiny – Law of Ukraine, 4, 66–75* [in Ukrainian].

19. Pohorets′kyy, M.A. (2013). Nehlasni slidchi (rozshukovi) diyi: problemy vprovadzhennya ta vykorystannya rezul′tativ u dokazuvanni. *Yurydychnyy chasopys Natsional'noyi akademiyi vnutrishnikh sprav Ukrayiny, 1, 270–276* [in Ukrainian].

20. Prysyazhnyuk, I. (2017). Dotrymannya prava na pryvatnist′ pry zdiysnenni sotsial′noho kontrolyu, spryamovanoho na protydiyu zlochynnosti. *Pravo Ukrayiny – Law of Ukraine, 12, 132–139* [in Ukrainian].

21. Prysyazhnyuk, I. (2017). Nedotorkannist′ pryvatnoho zhyttya yak ob″yekt kryminal′no-pravovoyi okhorony. *Pravo Ukrayiny – Law of Ukraine, 2, 131–138* [in Ukrainian].

22. Pro poshtovyy zv'yazok: Zakon Ukrayiny vid 4 zhovtnya 2011 r. № 2759-III. (2011). URL: http://zakon.rada.gov.ua/laws/show/2759-14.

23. Pro radiochastotnyy resurs Ukrayiny: Zakon Ukrayiny vid 1 chervnya 2000 r. № 1770-III. (2000). URL: http://zakon.rada.gov.ua/laws/show/1770-14.

24. Rishennya Konstytutsiynoho Sudu Ukrayiny u spravi za konstytutsiynym podannyam Zhashkivs′koyi rayonnoyi rady Cherkas′koyi oblasti shchodo ofitsiynoho tlumachennya polozhen′ chastyn pershoyi, druhoyi statti 32, chastyn druhoyi, tret′oyi statti 34 Konstytutsiyi Ukrayiny. (2012). URL: http://zakon4.rada.gov.ua/laws/show/ v002p710-12/print1389947652746863.

25. Serhyeyeva, D. (2014). Problemni aspekty vykorystannya rezul′tativ znyattya informatsiyi z transportnykh telekomunikatsiynykh merezh yak dokaziv u kryminal′nomu provadzhenni. *Pravo Ukrayiny – Law of Ukraine, 11, 209–218* [in Ukrainian].

26. Serhyeyeva, D. (2017). Vykorystannya rezul′tativ nehlasnykh slidchykh (rozshukovykh) diy dlya otrymannya okremykh vydiv dokaziv u kryminal′nomu provadzhenni: problemni pytannya. *Pravo Ukrayiny – Law of Ukraine, 12, 49–61* [in Ukrainian].

27. Ser′ohin, V. (2010). Zmist i obsyah prava na nedotorkannist′ pryvatnoho zhyttya (prayvesi). *Visnyk Akademiyi pravovykh nauk Ukrayiny, 4 (63), 88–97* [in Ukrainian].

28. Smartfon. Vikipediya: veb-sayt. (2020). URL: https://uk.m.wikipedia.org /wiki/Smartfon [in Ukrainian].

29. Sprava «Benedykt proty Sloveniyi» (povnyy tekst rishennya). (2018). URL: https://www.echr.com.ua/translation/sprava-benedik-proti-slovenii-povnij-tekst-rishennya/ [in Ukrainian].

30. Shevchyshen, A. (2016). Mozhlyvosti zbyrannya dokaziv i rozshuku pry zdiysnenni okremykh nehlasnykh slidchykh (rozshukovykh) diy u kryminal′nykh provadzhennyakh pro koruptsiyni zlochyny u sferi sluzhbovoyi ta profesiynoyi diyal′nosti, pov'yazanoyi z nadannyam publichnykh posluh. *Pravo Ukrayiny – Law of Ukraine, 10, 177–185* [in Ukrainian].

Панасюк А. А., Рак С. В., Булгакова Ю. Н. Отдельные вопросы надлежащей правовой процедуры осуществления доступа к частной информации во время производства досудебного расследования

В статье рассмотрены отдельные проблемы осуществления доступа к частной информации во время производства досудебного расследования уголовных правонарушений. Правовая защита персональных данных и права на частное общение исследовано в разрезе особенностей осуществления следственных, негласных следственных (розыскных), а также иных процессуальных действий в уголовном производстве, имеющих отношение к доступу к отдельным средствам телекомуникации.

***Ключевые слова**: защита права на приватность, вмешательство в частное общение, средства телекомуникации, негласные следственные (розыскные) действия, допустимость доказательств, надлежащая правовая процедура, смартфон.*

Panasiuk O. A., Rak S. V., Bulhakova J. N. Some Issues of Due Process of Access to Private Information at the Pretrial Investigation

The problem issues of get and accomplish access to private information at the pretrial investigation are analyzed in the paper. Law protection of personal data and right to privacy are researching in the context of peculiarities of conducting investigative (search), secret investigative (search) and other procedural actions in criminal proceedings, which concern with access to some telecommunication means.

Key words*: protection of right to privacy, interference in private communication, telecommunication means, secret investigative (search) actions, admissibility of evidence, due process, smartphone*.