

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

**ВИКОРИСТАННЯ ІНФОРМАЦІЇ, ЩО ЗНАХОДИТЬСЯ В
ОПЕРАТОРІВ ТА ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ У
КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ**

Методичні рекомендації

Київ 2021

Авторський колектив:

Таран О.В., доктор юридичних наук, професор (Національна академія внутрішніх справ); **Брисковська О.М.**, кандидат юридичних наук, старший науковий співробітник (Національна академія внутрішніх справ); **Тарасенко О.С.**, кандидат юридичних наук, доцент (Національна академія внутрішніх справ); **Вознюк А.А.**, доктор юридичних наук, професор (Національна академія внутрішніх справ); **Запотоцький А.П.**, доктор юридичних наук, професор (Національна академія внутрішніх справ); **Мотиль В.І.**, кандидат юридичних наук, старший науковий співробітник (Національна академія внутрішніх справ)

Рецензенти:

Шевчишен А. В., доктор юридичних наук, доцент, начальник відділу розслідування службових злочинів управління розслідування корупційних злочинів Головного слідчого управління Національної поліції України;

Швець М. Я., доктор економічних наук, професор, провідний науковий співробітник наукової лабораторії з проблем пономічнихротидії злочинності ННІ № 1 Національної академії внутрішніх справ

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ від 26 листопада 2021 р. (протокол № 3)

В 433 Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні [Текст]: метод. рек. / [О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін.]. – Київ: Нац. акад. внутр. справ, 2021. – 50 с.

У методичних рекомендаціях розкрито поняття телекомунікацій, види телекомунікаційних послуг, проаналізовано законодавче регулювання діяльності операторів і провайдерів телекомунікацій у контексті вирішення завдань кримінального провадження, визначено особливості здійснення тимчасового доступу до речей і документів, які знаходяться в операторів та провайдерів телекомунікацій, а також проведення негласних слідчих (розшукових) дій (ст. 263, 264, 268 КПК України).

Для слідчих та практичних працівників інших підрозділів ОВС, прокуратури, суду, а також науковців, викладачів та курсантів.

ЗМІСТ

Вступ	4
1. Поняття телекомунікацій, види телекомунікаційних послуг, законодавче регулювання діяльності операторів і провайдерів телекомунікацій у контексті вирішення завдань кримінального провадження	6
2. Тимчасовий доступ до речей і документів, які знаходяться в операторів та провайдерів телекомунікацій	11
3. Зняття інформації з транспортних телекомунікаційних мереж	17
4. Зняття інформації з електронних інформаційних систем	24
5. Установлення місцезнаходження радіоелектронного засобу	28
6. Право співробітника оперативного підрозділу на ознайомлення та отримання інформації від провайдера телекомунікаційних послуг	31
Додатки	34
Список використаних джерел	47

ВСТУП

Телекомунікації відіграють значну роль у будь-якій сучасній діяльності та процесах, цей динамічний соціально-економічний сектор забезпечує передавання інформації, що розширює межі спілкування, розвиток економіки та впливає на всі сфери життя.

Географічні межі ринку телекомунікацій є загальнодержавними, включають територію всієї країни, де надаються послуги з надання у користування місцевих, міжміських та міжнародних каналів електрозв'язку. Для зазначеного ринку послуг з надання у користування каналів електрозв'язку кінцевими споживачами виступають фізичні та юридичні особи, які замовляють такі послуги у оператора телекомунікацій, що отримав право на здійснення діяльності у сфері телекомунікацій¹.

Таким чином, телекомунікації є основою системи спілкування і передавання інформації, що поєднує широке коло суб'єктів. Можливості такої системи застосовуються у кримінальному провадженні задля забезпечення його дієвості.

Інформація, що знаходиться в операторів та провайдерів телекомунікацій має суттєве значення у кримінальному провадженні, оскільки, встановивши, хто саме користувався послугами операторів мобільного зв'язку, слідством може бути отримано інформацію про особу правопорушника, його зв'язки та протиправну діяльність.

Отримані в оператора телекомунікацій відомості можуть бути використані як докази у кримінальному провадженні.

Відповідно до ч. 4 ст. 39 Закону України «Про телекомунікації» від 01.07.2010 року № 2392-6 оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів і забезпечувати ці технічні засоби, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення.

Згідно зі ст. 9 вказаного Закону зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом.

Статтею 34 ч. 3 Закону України «Про телекомунікації» передбачено, що інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватися у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача.

Отже, отримання і використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні є важливим засобом забезпечення виконання його завдань, а саме – захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також

¹ Звіт за результатами аналізу ринку послуг з надання у користування каналів електрозв'язку зі швидкістю до 2 Мбіт/с кінцевим споживачам. Додаток до рішення НКРЗІ від 26.10.2021 р. № 403.

забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура.

У методичних рекомендаціях розкрито поняття телекомунікацій, види телекомунікаційних послуг, проаналізовано законодавче регулювання діяльності операторів і провайдерів телекомунікацій у контексті вирішення завдань кримінального провадження, визначено особливості здійснення тимчасового доступу до речей і документів, які знаходяться в операторів та провайдерів телекомунікацій, а також проведення негласних слідчих (розшукових) дій (ст.263, 264, 268 КПК України).

1. Поняття телекомунікацій, види телекомунікаційних послуг, законодавче регулювання діяльності операторів і провайдерів телекомунікацій у контексті вирішення завдань кримінального провадження

Відповідно до статті 14 КПК України «Таємниця спілкування», під час кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених цим Кодексом, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети. Інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального провадження.

Статтею 15 КПК України «Невтручання у приватне життя» передбачено, що під час кримінального провадження кожному гарантується невтручання у приватне (особисте і сімейне) життя. Ніхто не може збирати, зберігати, використовувати та поширювати інформацію про приватне життя особи без її згоди, крім випадків, передбачених цим Кодексом. Інформація про приватне життя особи, отримана в порядку, передбаченому цим Кодексом, не може бути використана інакше як для виконання завдань кримінального провадження. Кожен, кому наданий доступ до інформації про приватне життя, зобов'язаний запобігати розголошенню такої інформації.

Наведені положення кореспондуються зі ст. 8 Конвенції про захист прав і основоположних свобод людини та ст. 31, 32 Конституції України, а їх визначення як засад кримінального провадження свідчить про визнання пріоритету прав людини і обов'язок уповноважених суб'єктів діяти у спосіб, передбачений законом.

Отже, у кримінальному провадженні визначені випадки та умови отримання і використання певних особистих даних та інформації у тому числі тих, що передаються/приймаються за допомогою телекомунікацій.

Сфера телекомунікацій є складовою частиною галузі зв'язку України. Телекомунікації є невід'ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах (ст. 3 Закону України «Про телекомунікації»).

Нормативною основою надання та отримання телекомунікаційних послуг, регулювання відносин між операторами, провайдерами телекомунікацій та споживачами послуг є Закони України «Про телекомунікації», «Про телебачення і радіомовлення», «Про радіочастотний ресурс України», «Про захист прав споживачів», «Про захист персональних даних», «Правила надання та отримання телекомунікаційних послуг» інші нормативно-правові акти, що

встановлюють загальний порядок надання та отримання телекомунікаційних послуг.

Необхідність виконання завдань кримінального провадження досить часто обумовлює втручання у таємницю спілкування і приватне життя. Це втручання має бути правомірним, необхідним і пропорційним, щоб не становити порушення прав людини. Такі вимоги концептуально витікають з ч. 3 ст. 14 та ч. 3 ст. 15 КПК України: інформація про приватне життя особи та інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше, як для виконання завдань кримінального провадження.

Стрімкий технологічний розвиток і прискорення всіх процесів обумовлюють зміну підходів до поняття «спілкування» та «приватність». Автоматизація і комп'ютеризація процесів, технократизація і діджиталізація суспільства сприяють тому, що значні масиви інформації в повідомленнях приватного (особистого) характеру зберігаються на віддалених серверах (в т.ч. з доступом через «хмарні» технології) або в електронних інформаційних (телекомунікаційних) системах.

Останнім часом електронне листування майже витіснило письмову форму кореспонденції, а основним засобом комунікації в мережі Інтернет стало використання мережевих служб, що дозволяють користувачам обмінюватися повідомленнями або документами без застосування паперових носіїв (електронної пошти). Згідно ст. 1 Закону України «Про інформацію», будь-які відомості та/або дані, які можуть бути відображені в електронному вигляді, належать до інформації з розповсюдженням на них відповідних гарантій¹.

Сучасні телекомунікаційні засоби та послуги різноманітні і широко використовуються. До основних з них належать:

надання послуг фіксованого місцевого телефонного зв'язку – послуги телефонії будь-якому абоненту телекомунікаційної мережі загального користування (ТМЗК), яка забезпечує йому зв'язок з абонентами телекомунікаційних мереж однієї і тієї самої зони нумерації та (в тому числі) отримання загальнодоступних телекомунікаційних послуг;

надання послуг фіксованого міжміського телефонного зв'язку – послуги телефонії будь-якому абоненту ТМЗК, яка забезпечує йому зв'язок з абонентами телекомунікаційних мереж різних зон нумерації;

надання послуг фіксованого міжнародного телефонного зв'язку – послуги телефонії будь-якому абоненту ТМЗК, яка забезпечує йому зв'язок з абонентами телекомунікаційних мереж різних країн;

надання глобальних телекомунікаційних послуг – послуги телефонного зв'язку широкого вжитку в мережах різних операторів і провайдерів, до яких всі абоненти телефонної мережі загального користування мають вільний доступ і яка надається за кодами послуг 800 «виклик за рахунок абонента, якого викликають» та 900 «з розподілом прибутків»;

¹ Михайленко В., Островська О. Питання тимчасового доступу до вмісту електронної поштової скриньки. URL: <https://ur-gazeta.com/publications/practice/inshe/pitannya-timchasovogo-dostupu-do-vmistu-elektronnoyi-poshtovoyi-skrinky.html>.

надання голосових послуг у мережі рухомого (мобільного) зв'язку – послуги обміну інформацією голосом у реальному часі з використанням мережі рухомого (мобільного) зв'язку, під час отримання яких кінцеве обладнання абонента може вільно переміщатися в межах мережі оператора або його роумінг-партнера із збереженням абонентського номера або мережевого ідентифікатора споживача;

надання послуг доступу до Інтернету та передавання даних в мережі рухомого (мобільного) зв'язку – послуги, які забезпечують доступ будь-якому користувачу до інформаційних ресурсів, розміщених в Інтернеті, передавання інформації у вигляді даних з використанням мережі рухомого (мобільного) зв'язку, під час отримання яких кінцеве обладнання абонента може вільно переміщатися в межах мережі оператора або його роумінг-партнера із збереженням абонентського номера або мережевого ідентифікатора споживача;

надання послуг проводового доступу до Інтернету споживачам – забезпечення можливості з'єднання кінцевого обладнання споживача з Інтернетом з використанням підключення до проводової мережі за допомогою мідного або коаксіального кабелю, оптоволоконного підключення;

надання послуг безпроводового доступу до Інтернету споживачам – забезпечення можливості з'єднання кінцевого обладнання споживача з Інтернетом з використанням безпроводового доступу за радіотехнологіями, дозволеними Планом використання радіочастотного ресурсу України;

надання послуг доступу до Інтернету операторам, провайдерам телекомунікацій, в т.ч. IP-транзит – надання послуг доступу до Інтернету, в т.ч. IP-транзит, операторам, провайдерам телекомунікацій для надання послуг власним споживачам або іншим операторам, провайдерам;

надання послуг супутникового зв'язку – послуги рухомого або фіксованого зв'язку з використанням радіотехнологій, що базуються на використанні штучних супутників Землі;

надання послуг рухомого зв'язку: ультракороткохвильового, транкінгового – послуги із застосуванням радіотехнологій ультракороткохвильового або транкінгового зв'язку, під час отримання яких кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах телекомунікаційної мережі оператора із збереженням абонентського номера або мережевого ідентифікатора споживача;

надання послуг доступу до інфраструктури телекомунікаційних мереж, у тому числі надання в користування кабельної каналізації електрозв'язку, ліній зв'язку (в т.ч. волоконно-оптичних), елементів інфраструктури – послуги забезпечення спільного користування інфраструктурою/елементами інфраструктури, надання в користування інфраструктури (пасивної та/або активної) телекомунікаційних мереж, а також надання в користування кабельної каналізації електрозв'язку;

надання в користування каналів електрозв'язку (у тому числі каналів передавання даних) іншим операторам, провайдерам телекомунікацій, споживачам – послуги надання в користування каналів електрозв'язку, організованих за будь-якою технологією;

надання послуг передавання сигналів у телекомунікаційних мережах для потреб телерадіоорганізацій – послуги із приймання/передавання інформаційних продуктів та інформаційних послуг з використанням технічних засобів телекомунікацій на замовлення телерадіоорганізацій;

надання послуг технічного обслуговування і експлуатації телекомунікаційних мереж – послуги з підтримки у працездатному стані обладнання телекомунікаційних мереж в процесі його експлуатації, при якому воно здатне виконувати задані функції, зберігаючи задані значення параметрів у межах, які встановлені в нормативно-технічній документації; експлуатація телекомунікаційних мереж.

Загальне поняття «телекомунікації», що надається у Законі України «Про телекомунікації» розкриває способи спілкування із використанням телекомунікацій, його форми та шляхи і визначається як передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.

Таким чином, у кримінальному провадженні у передбачених законом випадках можливе отримання інформації та даних, що передаються/приймаються за допомогою телекомунікацій і є продуктом діяльності оператора та/або провайдера телекомунікацій, що спрямований на задоволення потреб споживачів у сфері телекомунікацій.

Для виконання завдань кримінального провадження зміст такої інформації можуть становити відомості про:

з'єднання – установа зв'язку між кінцевими обладнаннями абонентів для обміну інформацією;

зону дії телефонної станції (підстанції) – територія, на якій забезпечується надання послуг споживачам, яким присвоєно телефонний номер такої станції (підстанції);

електронний код (ідентифікатор) кінцевого обладнання – код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо);

ідентифікаційну телекомунікаційну картку – засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо);

картку попередньо оплаченої послуги – засіб для замовлення та попередньої оплати послуг, що дає право споживачеві на отримання визначеного переліку та/або обсягу послуг оператора, провайдера в межах визначеного активу такого засобу;

картку поповнення рахунка – засіб поповнення особового рахунка абонента для оплати послуг оператора, провайдера в межах визначеного активу такого засобу;

конвергенцію телекомунікаційних мереж фіксованого та рухомого (мобільного) зв'язку – спільне використання операторами, провайдерами телекомунікацій елементів інфраструктури та ресурсів телекомунікаційних

мереж фіксованого та рухомого (мобільного) зв'язку для надання телекомунікаційних послуг споживачам;

мережевий ідентифікатор споживача – індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в телекомунікаційній мережі чи Інтернеті;

послуги рухомого (мобільного) зв'язку – послуги, які надаються оператором рухомого (мобільного) зв'язку і під час отримання яких кінцеве обладнання абонента може вільно переміщатися в межах телекомунікаційної мережі такого оператора або його роумінг-партнера із збереженням абонентського номера або мережевого ідентифікатора споживача;

роумінг – послуга, яка забезпечує можливість абонентові одного оператора рухомого (мобільного) зв'язку отримувати послуги в мережі іншого оператора із збереженням початкової реєстрації абонента в телекомунікаційній мережі свого оператора;

сеанс зв'язку – процес надання та отримання послуги з моменту встановлення з'єднання до його завершення;

спарену схему включення кінцевого обладнання абонентів – спосіб включення кінцевого обладнання двох абонентів з двома різними абонентськими номерами в одну абонентську лінію, при якому з'єднання можливе тільки по черзі для кожного з них;

телефонний зв'язок – вид електрозв'язку для передачі голосових повідомлень у реальному часі з використанням номерного ресурсу телефонної мережі та ін.

Суб'єктами, які здійснюють діяльність у сфері телекомунікацій, а отже, можуть надати відповідну інформацію та дані є оператори і провайдери телекомунікацій.

Оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж.

Провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

Особа щодо якої у межах кримінального провадження може виникнути необхідність отримання інформації та даних, які були передані/прийняті із застосуванням телекомунікацій є споживачем телекомунікаційних послуг – це юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб.

Оператори, провайдери, споживачі, виробники та/або постачальники технічних засобів телекомунікацій є суб'єктами ринку телекомунікацій.

Реєстр операторів, провайдерів телекомунікацій доступний на офіційному сайті Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за посиланням <https://nrzi.gov.ua/index.php?r=site/index&pg=55&language=uk>.

Відповідно до ч. 2 ст. 39 Закону України «Про телекомунікації» оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом. А у ч. 4 цієї статті передбачено, що оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових та розвідувальних заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових та розвідувальних заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

Таким чином, законодавством визначені обов'язки операторів телекомунікацій забезпечувати збереження та передавання інформації, а також створити умови для діяльності правоохоронних органів у випадках, передбачених законом.

Отримання інформації, що знаходиться в операторів та провайдерів телекомунікацій для виконання завдань кримінального провадження відбувається у межах здійснення тимчасового доступу до речей і документів та за допомогою проведення негласних слідчих (розшукових) дій.

2. Тимчасовий доступ до речей і документів, які знаходяться в операторів та провайдерів телекомунікацій

Тимчасовий доступ до речей і документів є заходом забезпечення кримінального провадження, порядок отримання дозволу та умови його здійснення передбачені нормами КПК України і підлягають системному застосуванню.

Законодавством визначені умови надання дозволу на проведення цього заходу забезпечення кримінального провадження, доказування яких покладається на сторону кримінального провадження, яка звертається з відповідним клопотанням. Так, відповідно до вимог ч.5 ст.163 КПК України слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи:

1) перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;

2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні;

3) не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю.

Відповідно до ст. 162 КПК України до охоронюваної законом таємниці, яка міститься в речах і документах, належать: 1) інформація, що знаходиться у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації; 2) відомості, які можуть становити лікарську таємницю; 3) відомості, які можуть становити таємницю вчинення нотаріальних дій; 4) конфіденційна інформація, в тому числі така, що містить комерційну таємницю; 5) відомості, які можуть становити банківську таємницю; 6) особисте листування особи та інші записи особистого характеру; 7) інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 8) персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних; 9) державна таємниця; 10) таємниця фінансового моніторингу.

За змістом ч. 3 ст. 132 КПК України застосування заходів забезпечення кримінального провадження не допускається, якщо слідчий, прокурор не доведе, що: 1) існує обґрунтована підозра щодо вчинення кримінального правопорушення такого ступеня тяжкості, що може бути підставою для застосування заходів забезпечення кримінального провадження; 2) потреби досудового розслідування виправдовують такий ступінь втручання у права і свободи особи, про який ідеться в клопотанні слідчого, прокурора; 3) може бути виконане завдання, для виконання якого слідчий, прокурор звертається із клопотанням.

Під час розгляду питання про застосування заходів забезпечення кримінального провадження сторони кримінального провадження повинні подати слідчому судді або суду докази обставин, на які вони посилаються (ч.5 ст.132 КПК України).

Відповідно до ч. 7 ст. 163 КПК України слідчий суддя, суд в ухвалі про надання тимчасового доступу до речей і документів може дати розпорядження про надання можливості вилучення речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що без такого вилучення існує реальна загроза зміни або знищення речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів.

Ухвала надається оператору або провайдеру телекомунікацій, у володінні яких знаходиться необхідна інформація, після чого відповідна службова особа зобов'язана надати тимчасовий доступ до зазначеної в ній інформації, з метою вилучення необхідної інформації (її носіїв, тощо про що зазначається в ухвалі слідчого судді, суду) або виготовлення необхідних копій; слідчий аналізує отримані дані або дає доручення оперативним підрозділам на їх моніторинг. У подальшому отримана інформація (щодо абонентського номера оператора мобільного зв'язку) аналізується та в разі необхідності отримання додаткової інформації, яка має значення для кримінального провадження, можливе

проведення негласних слідчих (розшукових) дій, таких як, наприклад, зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) або ж установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України)¹.

Тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання тощо і не дають можливості втрутитися у приватне спілкування, тобто отримати доступ до змісту інформації, що передається.

У статтях 159, 162 КПК передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), у тому числі про місцезнаходження радіоелектронного засобу у певний день та час.

Особа, зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана згідно з ч.1 ст.165 КПК надати тимчасовий доступ до визначених в ухвалі речей або документів особі, вказаній у відповідній ухвалі слідчого судді, суду або ж особі, уповноваженій на здійснення тимчасового доступу на підставі доручення слідчого. Ураховуючи специфіку формату зберігання інформації, що передбачена у п.7 ч.1 ст.162 КПК і знаходиться в операторів (провайдерів) телекомунікацій, надання доступу до відповідних документів (тобто надання можливості ознайомитися з ними та зробити з них копії) може здійснюватися як безпосередньо в оператора (провайдера), так і шляхом надання доступу до відповідних документів уповноваженому на зняття інформації з транспортних телекомунікаційних мереж підрозділу правоохоронного органу через відповідні інформаційні системи відповідно до встановленого порядку з обов'язковим наданням копії ухвали слідчого судді відповідному оператору (провайдеру).

ЄСПЛ у своїх рішеннях неодноразово розглядав питання щодо надання доступу до речей та документів в рамках кримінального провадження. Те, чи потрапляють такі питання у сферу дії Конвенції повністю залежить від того, до якої інформації чи речей надається доступ. Зазвичай у справах, які були розглянуті ЄСПЛ, мова йшла про:

доступ до інформації про з'єднання абонента (див. рішення у справах «*Malone v. The United Kingdom*», заява № 8691/79; «*Ben Faiza c. France*», заява № 31446/12);

інформації про стан здоров'я (див. рішення у справах «*L.H. v. Latvia*» заява № 52019/07 та «*Avilkina and Others v. Russia*», заява № 1585/09); та

банківської інформації (див. рішення у справі «*M.N. and Others v. San Marino*», заява № 28005/12).

Оскільки вказана інформація стосується приватного життя особи (фактично йдеться про збір персональних даних чутливого характеру), надання до неї доступу становитиме, на думку ЄСПЛ, втручання в права, гарантовані статтею 8 Конвенції («Право на повагу до приватного і сімейного життя»).

¹ Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в Україні. Вісник ЛДУВС ім. Е.О. Дідоренка. 2017. № 2. С. 118.

У вказаних рішеннях, а також численних інших рішеннях щодо збору / надання доступу до інформації про особу (див., наприклад, узагальнення практики з цього приводу в рішенні у справі «*Roman Zakharov v. Russia*», заява № 47143/06) ЄСПЛ сформулював детальні критерії, яким повинно відповідати таке втручання:

- інформація збирається на підставі закону;
- положення закону відповідають вимогам доступності, чіткості та передбачуваності;
- прийняття рішень щодо надання доступу повинні бути предметом судового контролю;
- такий контроль повинен передбачати можливість особі навести свої аргументи;
- рішення суду повинно бути обґрунтованим;
- вказівки в ухвалі суду щодо того, до якої інформації (документів) надається доступ, повинні бути максимально чіткими;
- особа, інформація щодо якої передається, повинна володіти ефективними засобами захисту, що передбачали б можливість оскарження законності та обґрунтованості отримання доступу до такої інформації, а також отримання компенсації в разі виявлення порушення;
- доступ повинен надаватися лише до інформації, що необхідна для цілей розслідування;
- отримана інформація повинна належним чином фіксуватися, зберігатися та захищатися, щоб запобігати її модифікації, незаконному знищенню та поширенню;
- отримана інформація повинна невідкладно знищуватися в разі зникнення подальшої в ній потреби.

Недотримання вказаних правил тягтиме за собою констатацію ЄСПЛ порушення прав особи, гарантованих статтею 8 Конвенції¹.

Узагальнення правозастосовної практики показало, що під час кримінального провадження уповноважені суб'єкти ініціюють проведення тимчасового доступу до речей і документів і звертаються до слідчого із клопотанням про отримання відповідного дозволу, де предметом запиту зазвичай є:

- ідентифікаційні ознаки кінцевого обладнання (абонентський номер, міжнародний ідентифікатор кінцевого обладнання (IMEI), яке перебувало у зоні дії базових станцій (абонента);
- адреси розташування та номери базових станцій, які забезпечували зв'язок кінцевого обладнання абонента;
- типи з'єднань абонента: вхідні та вихідні дзвінки, SMS (короткі текстові повідомлення: абонентський номер отримувача та відправника, час, дата, місце), MMS (мультимедійні повідомлення: абонентський номер отримувача та відправника, час, дата, місце), GPRS (передача інформації по незайнятій

¹ Бем М. Отримання доступу до речей і документів у світлі практики ЄСПЛ. URL: <https://vkr.ua/publication/otrimannya-dostupu-do-rechey-i-dokumentiv-u-svitli-praktiki-iespl>.

голосовим зв'язком смузї частот: абонентський номер отримувача та відправника, час, дата, місце), переадресація;

– дата, час та тривалість з'єднань, у тому числі з'єднань нульової тривалості (неприйняті виклики) абонента;

– ідентифікаційні ознаки кінцевого обладнання (абонентський номер, ІМЕІ), з яким відбувся сеанс зв'язку абонента, а також, за наявності контрактної угоди, (відповідної реєстрації) з абонентом, відомості про його особу.

Інформація, отримана за результатами здійснення тимчасового доступу до речей і документів може бути використана для:

визначення місця знаходження телефону та маршрутів його переміщення (для цього використовуються ідентифікатори базових станцій мобільних операторів (LAC і CID), а запити з кількох базових станцій можуть допомогти встановити місцезнаходження пристрою з максимальною точністю,

встановлення факту та кола спілкування абонентів;

тривалість з'єднань (включно нульові);

сервісні sms, назва яких може містити інформацію про певні дії та ім'я абонента.

Отримання судового дозволу на здійснення тимчасового доступу до речей і документів, які знаходяться в операторів та провайдерів телекомунікацій залежить також від правильного розмежування цього заходу забезпечення кримінального провадження від негласних слідчих (розшукових) дій.

Так, як зазначено в ухвалі слідчого судді, в провадження слідчого судді надійшло клопотання старшого слідчого відділу з розслідування особливо важливих злочинів слідчого управління ГУНП в Полтавській області старшого лейтенанта поліції ОСОБА_1 про дозвіл на тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, погоджене прокурором відділу прокуратури Полтавської області ОСОБА_2 В якому прохали: Надати тимчасовий доступ до інформації про зв'язок кінцевих обладнань споживачів телекомунікаційних послуг, здійснених через ТОВ «ЛАЙФСЕЛЛ»; ПрАТ «Київстар»; ПрАТ «ВФ Україна». Зобов'язати ТОВ «ЛАЙФСЕЛЛ»; ПрАТ «Київстар»; ПрАТ «ВФ Україна» виготовити на паперовому та/або електронному носії документ за вказаними вище координатами та періодом часу з 08:00 год. 16.01.2017 по 18:00 год. 16.01.2017 року з наступними відомостями: ПрАТ «Київстар» LAC 54703 CID 21081741, 21081831, 21081731;LAC 54713 CID 21096331, 21096333; LAC 44403 CID 171, 11783, 8181, 11782, 8171, 182, 10358, 20358, 30358;LAC 56403 CID 9631.ПрАТ «ВФ Україна»LAC17051CID 30183, 30187, 30402, 30406, 39045,39047, 30401, 11409, 11406, 22283, 11403,135686945, 135686985, 135710495, 135689760,135689504, 135700511, 135689544.ТОВ «ЛАЙФСЕЛЛ» LAC 23303 CID 2361, 2363, 2362, 2123, 813, 2121,16931, 16932, 16933, 91023611, 91023613,91021234, 91021214;LAC 23301 CID 887. Ідентифікаційні ознаки кінцевого обладнання (абонентський номер, міжнародний ідентифікатор кінцевого обладнання (далі – ІМЕІ), яке перебувало у зоні дії базових станцій (абонент А). Адреси розташування та номери базових станцій, які

забезпечували зв'язок абонентів ОСОБА_3 з'єднання абонентів А: вхідні та вихідні дзвінки, SMS (короткі текстові повідомлення), MMS (мультимедійні повідомлення), GPRS (передача інформації по незайнятій голосовим зв'язком смузі частот), переадресація тощо. Дата, час та тривалість з'єднань, у тому числі з'єднання нульової тривалості (неприйняті виклики) абонентам А. Ідентифікаційні ознаки кінцевого обладнання (абонентський номер, ІМЕІ), з яким відбувався сеанс зв'язку абонентів А (абоненти Б).

Згідно зі ст.162 КПК України, передбачено спеціальний порядок доступу до речей і документів, які містять охоронювану законом таємницю, а саме отримання судового дозволу на підставі вмотивованого клопотання про тимчасовий доступ до речей та документів.

Згідно з п.7 ч.1 ст.162 КПК України, до охоронюваної законом таємниці, яка міститься в речах і документах, належить: інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Абонент – споживач телекомунікаційних послуг, який їх отримує на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі.

У зв'язку з можливістю такого широкого доступу до інформації про особу на практиці виникає проблема меж співвідношення процесуальної дії тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, та можливості проведення певних видів негласних слідчих (розшукових) дій.

Зокрема, у ст.159 та п.7 ч.1 ст.162 КПК України, передбачено такий захід забезпечення кримінального провадження, як тимчасовий доступ до документів, які знаходяться в операторів та провайдерів телекомунікацій та містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання, а ст.ст.263 та 268 КПК України, передбачено такі негласні слідчі (розшукові) дії, як зняття інформації з транспортних телекомунікаційних мереж та установами місцезнаходження радіоелектронного засобу відповідно. Зазначені процесуальні дії слід відмежовувати таким чином: дії, передбачені ст. ст. 263 та 268 КПК, є негласними слідчими (розшуковими) діями, дозвіл на проведення яких надає слідчий суддя суду апеляційної інстанції. Інформація щодо цих дій згідно із ЗУ "Про державну таємницю" та п.п. 4.12.4 і 4.12.5 Зводу відомостей, що становлять державну таємницю, затвердженого наказом СБ України від 12.08.2005 № 440, містить відомості, що становлять державну таємницю. Водночас дії, передбачені ст.159, п.7 ч.1 ст.162 КПК України, є заходами забезпечення кримінального провадження, дозвіл на застосування яких надає слідчий суддя суду першої інстанції, при цьому відомості щодо таких дій не становлять державної таємниці; тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні

з'єднання, SMS, MMS тощо), маршрути передавання тощо і не дають можливості втрутитися у приватне спілкування, тобто отримати доступ до змісту інформації, що передається. А зняття інформації з транспортних телекомунікаційних мереж (ст.263 КПК України) є різновидом втручання у приватне спілкування, оскільки здійснюється доступ до змісту повідомлень будь-якого виду та інформації, що передається особою під час зв'язку; у ст.ст.159, 162 КПК України передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), у тому числі про місцезнаходження радіоелектронного засобу у певний день та час. Водночас визначена у ст.268 КПК України, негласна слідча (розшукова) дія – установлення місцезнаходження радіоелектронного засобу – передбачає локалізацію (моніторинг) місцезнаходження радіоелектронного засобу в режимі реального часу (тобто дає змогу отримати інформацію про те, де перебуває відповідний засіб на момент спостереження за ним, визначити маршрут його перебування).

На підставі викладеного, приходжу до висновку відмовити у задоволенні клопотання, оскільки вимоги, які зазначаються у клопотанні, стосуються фактично негласних слідчих (розшукових) дій, зокрема, встановлення місцезнаходження радіоелектронного засобу, втручання в приватне спілкування, оскільки в клопотанні ставиться питання про надання інформації щодо невстановленого кола осіб, а не відносно конкретного абонента¹.

Узагальнення судової практики та типові недоліки щодо клопотань про тимчасовий доступ до речей і документів наведено в додатках.

3. Зняття інформації з транспортних телекомунікаційних мереж

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 р. № 114/1042/516/1199/936/1687/5.

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

¹ Ухвала Ожтєбрьського районного суду м. Полтави від 17.01.2019 р. у справі № 554/1862/18. Провадження №1-кв/554/1132/2019. Єдиний державний реєстр судових рішень. URL: <https://youcontrol.com.ua/ru/catalog/court-document/79267173/>

каналами зв'язку. Аналіз нормативно-правових актів кримінально-процесуального, оперативно-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 оперативно-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.

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 безпеки¹.

Об'єктом слідчої дії – зняття інформації з транспортних телекомунікаційних мереж може бути лише зміст розмов абонентів чи дані, якими вони обмінюються за допомогою транспортних телекомунікаційних мереж.

До інформації, яка може бути зафіксована з застосуванням цієї слідчої дії, належить інформація, яка передається технічними каналами зв'язку - телефоном, мобільними засобами телефонного, електронного чи радіозв'язку, за

¹ Бабкова В.С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України*. 2018. № 2 (37). С. 70–71.

допомогою комп'ютерної мережі зв'язку, включаючи засоби Інтернету: комп'ютерна телефонія [IP-phone], [e-mail], комп'ютерний пейджер [листування методом ICQ – обмін короткими текстовими повідомленнями в режимі реального часу шляхом набору тексту на клавіатурі комп'ютера] тощо. Розмови людей віч-на-віч (один на один) не можуть прослуховуватись в порядку проведення такої слідчої дії і не є її об'єктом.

До інформації, що підлягає фіксуванню з застосуванням процесуальної форми цієї слідчої дії, не належать дані операторів телефонних розмов та Інтернет-провайдерів щодо частоти та тривалості розмов абонентів, час перебування абонента в мережі зв'язку інша інформація технічного чи фінансового характеру. Така інформація може бути отримана шляхом наведення довідок.

Зняття інформації з транспортних телекомунікаційних мереж поділяється на:

– контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модем ний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється;

– зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Фактичні підстави зняття інформації з транспортних телекомунікаційних мереж – наявність достатніх підстав вважати, що в інформації, яка передається з застосуванням транспортних телекомунікаційних мереж від підозрюваного чи обвинуваченого іншим особам або від інших осіб підозрюваному чи обвинуваченому, а також у інформації, якою останні обмінюються за допомогою засобів зв'язку між собою, містяться дані про вчинений злочин і якщо іншими способами одержати ці дані неможливо.

Юридична підстава зняття інформації з транспортних телекомунікаційних мереж - ухвала слідчого судді.

За наявності необхідних підстав слідчий за погодженням з прокурором звертається з поданням до уповноваженого слідчого судді, який розглядає подання, вивчає матеріали провадження, за необхідності вислуховує слідчого, вислуховує думку прокурора, після чого залежно від підстав для прийняття такого рішення вносить ухвалу про зняття інформації з транспортних телекомунікаційних мереж або про відмову в цьому.

Згідно з ч. 4 ст. 39 Закону України «Про телекомунікації» оператори телекомунікацій зобов'язані встановлювати на своїх мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та

недопущенню розголошення організаційних і тактичних прийомів їх проведення, а також зобов'язані здійснювати захист зазначених технічних засобів від несанкціонованого доступу.

Слідчий вивчає зміст знятої інформації, про що складає протокол. Після виявлення даних, що мають доказове значення, в протоколі фіксується відповідна інформація, після чого слідчий своєю постановою визнає носій інформації доказом і приєднує його до провадження. Дослідження інформації, знятої з каналів зв'язку, у необхідних випадках проводиться з участю спеціаліста. Результати технічного документування телефонних розмов чи зняття інформації з інших технічних каналів зв'язку можуть мати значення доказів у провадженні за відповідності їх умовам належності до провадження, допустимості та достовірності.

Допустимими до використання як докази можуть бути лише такі матеріали, які одержані суб'єктом, уповноваженим на здійснення відповідної дії, одержані з винесеним відповідно до закону рішенням, одержані з дотриманням гарантованих Конституцією України гарантій недоторканості особистого життя людини та таємниці телефонних і інших розмов, самі матеріали всебічно досліджені, в тому числі експертами, і є достовірними, немає жодних сумнівів щодо наявності ознак монтажу.

Результати технічного документування мають бути ретельно перевірені і досліджені і лише за відповідності зафіксованої інформації вимогам достовірності можуть бути оприлюднені і використані як докази.

Для визначення достовірності фактичних матеріалів технічного документування може бути призначена – технічна експертиза матеріалів і засобів відео-звукозапису, чи експертиза телекомунікаційних систем та засобів, на розв'язання яких можуть бути поставлені питання: Чи є голос, зафіксований на фонограмі, голосом конкретної особи? Чи є ознаки механічного й електронного монтажу на фонограмі? Чи є ознаки втручання в роботу телекомунікаційної системи? тощо¹.

У спеціальній літературі сформульовано наступні висновки щодо питання допустимості доказів, отриманих за результатами зняття інформації з транспортних телекомунікаційних мереж.

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.

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

¹ Герасимчук А. Я. Зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України). Адвокат. URL: <https://www.facebook.com/advocate.mariupol/posts/269639480037047>.

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 особою участі у проведенні відповідної процесуальної дії не брала, може розглядатися як передумова визнання цього доказу недопустимим.

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 фоноскопічної експертизи¹.

Використання інформації, одержаної внаслідок зняття інформації з транспортних телекомунікаційних мереж можливе у іншому кримінальному провадженні.

Як зазначено в судовій ухвалі, До Київського апеляційного суду надійшло клопотання прокурора відділу Київської обласної прокуратури Беспалова О.С. про надання дозволу на передачу до СУ ГУ НП в Київській області інформації, одержаної внаслідок проведення негласних слідчих (розшукових) дій у кримінальному провадженні № 12019110000000537 від 25.07.2019, та використання її в іншому кримінальному провадженні №12021110000000243 від 03.03.2021. У відповідності до ч.ч. 1, 2 ст. 257 КПК України, якщо в результаті проведення негласної слідчої (розшукової) дії виявлено ознаки кримінального правопорушення, яке не розслідується у даному кримінальному провадженні, то отримана інформація може бути використана в іншому кримінальному провадженні тільки на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора. Слідчий суддя розглядає клопотання згідно з вимогами статей 247 та 248 цього Кодексу і відмовляє у його задоволенні, якщо прокурор, крім іншого, не доведе законність отримання інформації та наявність достатніх підстав вважати, що вона свідчить про виявлення ознак кримінального правопорушення.

Як убачається із матеріалів клопотання, слідчим управлінням ГУНП в Київській області здійснюється досудове розслідування у кримінальному провадженні внесеному до Єдиного реєстру досудових розслідувань за № 12019110000000537 від 25.07.2019 за ознаками кримінальних правопорушень, передбачених ч. 1, ч. 2 ст. 307 КК України. Досудовим розслідуванням встановлено, що громадянин ОСОБА_1 та ОСОБА_2 організували на території Бучанської виправної колонії збут наркотичних

¹ Бабкова В.С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України*. 2018. № 2 (37). С. 74.

засобів особам, які відбувають покарання у вказаній колонії. 02.12.2020 ОСОБА_2 вручено повідомлення про підозру у вчиненні ним кримінального правопорушення (злочину), передбаченого ч. 1 ст. 307 КК України, та цього ж дня ОСОБА_1 вручено повідомлення про підозру у вчиненні ним кримінального правопорушення (злочину), передбаченого ч. 1 ст. 307 КК України. 08.01.2021 ОСОБА_2 вручено повідомлення про зміну раніше повідомленої підозри та нову підозру у вчиненні ним кримінальних правопорушень (злочинів), передбачених ч. 1, ч. 2 ст. 307 КК України, та цього ж дня ОСОБА_1 вручено повідомлення про зміну раніше повідомленої підозри та нову підозру у вчиненні ним кримінальних правопорушень (злочинів), передбачених ч. 1, ч. 2 ст. 307 КК України. Крім того, у ході досудового розслідування кримінального провадження № 1201911000000537 встановлено, що на території Бучанської виправної колонії засуджений ОСОБА_3, ІНФОРМАЦІЯ_1, умисно встановив та поширював злочинний вплив, за вказаним фактом слідчим управлінням ГУНП в Київській області зареєстровано кримінальне провадження № 1202111000000243 від 03.03.2021 за ч. 2 ст. 255-1 КК України. У ході досудового розслідування у кримінальному провадженні № 1201911000000537 від 25.07.2019 у встановленому законодавством порядку проводились негласні слідчі (розшукові) дії, зокрема, на підставі ухвали Київського апеляційного суду № 01-45/824/5989/2020 від 05.03.2020 зі строком дії два місяці, щодо ОСОБА_3 проводились негласні слідчі (розшукові) дії, а саме зняття інформації з транспортних телекомунікаційних мереж. За результатами виконання ухвали суду про надання дозволу на проведення негласних слідчих (розшукових) дій складено протокол про результати проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 2638т/55/109-2020 від 14.07.2020 на 1 арк., прим. № 1; оптичний носій DVD-R, 4,7 Gb, інв. №507. Крім того, на підставі ухвали Київського апеляційного суду № 01-45/824/22440/2020 від 12.10.2020 зі строком дії два місяці, щодо ОСОБА_3 проводились негласні слідчі (розшукові) дії, а саме зняття інформації з транспортних телекомунікаційних мереж. За результатами виконання ухвали суду про надання дозволу на проведення негласних слідчих (розшукових) дій складено протокол про результати проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 48т/55/109-2021 від 05.01.2021 на 1 арк., прим. № 1; оптичний носій DVD-R, 4,7 Gb, інв. №1097. Також, на підставі ухвали Київського апеляційного суду № 01-45/824/16840/2020 від 23.07.2020 зі строком дії два місяці, щодо ОСОБА_3 проводились негласні слідчі (розшукові) дії, а саме зняття інформації з транспортних телекомунікаційних мереж. За результатами виконання ухвали суду про надання дозволу на проведення негласних слідчих (розшукових) дій складено протокол про результати проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 4604т/55/109-2020 від 05.11.2020 на 16 арк., прим. № 1; оптичний носій DVD-R, 4,7 Gb, інв. №1097. Вивченням матеріалів проведених негласних слідчих (розшукових) дій у кримінальному провадженні № 1201911000000537 від

25.07.2019 виявлено ознаки іншого кримінального правопорушення, яке не розслідується у даному кримінальному провадженні, як наслідок отримана інформація може бути використана у якості доказів в іншому кримінальному провадженні, а саме № 12021110000000243 від 03.03.2021 за ч. 2 ст. 255-1 КК України. Перевіривши доводи клопотання та матеріали досудового розслідування, заслухавши пояснення прокурора відділу Київської обласної прокуратури Беспалова О.С., який підтримав подане клопотання та просив його задовольнити, вважаю, що клопотання підлягає задоволенню в частині надання дозволу на використання у кримінальному провадженні № 12021110000000243 від 03.03.2021 результатів негласних слідчих (розшукових) дій, отриманих у кримінальному провадженні № 12019110000000537 від 25.07.2019, оскільки з матеріалів клопотання вбачається наявність достатніх підстав вважати, що результати негласних слідчих (розшукових) дій, отримані в межах досудового розслідування у кримінальному провадженні № 12019110000000537 від 25.07.2019, можуть бути використані як докази у кримінальному провадженні № 12021110000000243 від 03.03.2021. Разом з тим, задовольняючи вимоги прокурора в частині надання дозволу на використання результатів негласних слідчих (розшукових) дій в іншому кримінальному провадженні, слідчий суддя не убачає підстав для задоволення вимог прокурора про передачу до СУ ГУ НП в Київській області інформації, одержаної внаслідок проведення негласних слідчих (розшукових) дій у кримінальному провадженні № 12019110000000537 від 25.07.2019, оскільки чинним КПК України не передбачено повноважень слідчого судді на надання дозволу на передачу інформації, одержаної внаслідок проведення негласних слідчих (розшукових) дій у кримінальному провадженні. Керуючись ст. ст. 247-248, 257 КПК України, слідчий суддя, - Клопотання прокурора відділу Київської обласної прокуратури Беспалова Олексія Сергійовича про надання дозволу на передачу до СУ ГУ НП в Київській області інформації, одержаної внаслідок проведення негласних слідчих (розшукових) дій у кримінальному провадженні № 12019110000000537 від 25 липня 2019 року, та використання її в іншому кримінальному провадженні № 12021110000000243 від 03 березня 2021 року, задовольнити частково. Надати дозвіл на використання у кримінальному провадженні № 12021110000000243 від 03 березня 2021 року, результатів негласних слідчих (розшукових) дій, отриманих у кримінальному провадженні № 12019110000000537 від 25 липня 2019 року, а саме: протокол про результати проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 2638т/55/109-2020 від 14.07.2020 на 1 арк., не таємно; оптичний носій DVD-R, 4,7 Gb інв. № 507, одна одиниця, (розсекречено), який є додатком до протоколу про результати проведення негласної слідчої (розшукової) дії № 2638т/55/109-2020; протокол про результати проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 48т/55/109-2021 від 05.01.2021 на 1 арк., не таємно; оптичний носій DVD-R, 4,7 Gb інв. № 1097, одна одиниця, (розсекречено), який є додатком до протоколу про результати проведення негласної слідчої (розшукової) дії № 48т/55/109-2021; протокол про результати проведення негласної слідчої

(розшукової) дії, а саме зняття інформації з транспортних телекомунікаційних мереж № 4604т/55/109-2020 від 05.11.2020 на 16 арк., не таємно; оптичний носій DVD-R, 4,7 Gb інв. № 1097, одна одиниця, (розсекречено), який є додатком до протоколу про результати проведення негласної слідчої (розшукової) дії № 4604т/55/109-2020¹.

4. Зняття інформації з електронних інформаційних систем

Відповідно до п.8 ч.1 ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах, інформаційна система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Таким чином, до інформаційних систем відноситься комп'ютерна техніка, мобільні телефони, планшети та інші пристрої, які використовуються для обробки інформації з використанням програмних засобів².

Під електронною інформаційною системою слід розуміти взаємозв'язок технічних засобів (комп'ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп'ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному вигляді. В той же час, під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту.

Сутність зняття інформації з електронних інформаційних систем полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частинах, без відома власника, володільця або утримувача системи. Зазначена НСРД проводиться, у разі якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися, як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення. Негласне зняття інформації з засобів електронно-обчислювальної техніки полягає у застосуванні технічних засобів із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диску (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого. Програмне проникнення до

¹ Ухвала Київського апеляційного суду від 16 берез. 2021 року. URL: <https://vkursi.pro/vsudi/decision/95595884>.

² Особливості проведення негласних слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень. URL: <https://sa.dn.ua/osoblivosti-provedennya-neglasnikh-sl/3/>

електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують подолання системи захисту і копіювання інформації, що обробляється в зазначених системах (їх частинах), на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю НСРД¹.

Важливим є процесуальний порядок прийняття рішення про застосування такої негласної слідчої (розшукової) дії. В ухвалі слідчого судді про дозвіл на негласне втручання у приватне спілкування додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, у яку може здійснюватися втручання у приватне спілкування (найменування електронної інформаційної системи, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець або утримувач) та спосіб, яким обмежений доступ до неї. Ідентифікаційними ознаками електронної інформаційної системи є:

– IP-адреса (IP-Internet Protocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету;

– доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти;

– серійний номер та характеристики автоматизованої системи та ЕОМ².

Всі способи зняття інформації з електронних інформаційних систем можна об'єднати в дві основні групи. Перша група — це способи безпосереднього доступу. При їх реалізації інформація отримується шляхом видачі відповідних команд з комп'ютера, на якому ця інформація знаходиться. Друга група включає способи опосередкованого (віддаленого) доступу до комп'ютерної інформації. До них можна віднести:

підключення до лінії зв'язку користувача (наприклад, до телефонної лінії або оптоволоконної лінії) і отримання цим шляхом доступу до електронної інформаційної системи;

проникнення в комп'ютерну систему за допомогою підбору паролів тощо.

До числа способів опосередкованого (віддаленого) доступу до комп'ютерної інформації належать способи безпосереднього та електромагнітного перехоплення. Безпосереднє перехоплення – найпростіший спосіб доступу до електронної інформаційної системи. Перехоплення здійснюється або прямо через зовнішні комунікаційні канали системи, або шляхом безпосереднього підключення до ліній периферійних пристроїв. При цьому об'єктами безпосереднього перехоплення є кабельні і провідні системи, наземні мікрохвильові системи, системи урядового зв'язку. Зокрема, електромагнітне перехоплення являється досить цікавою річчю в руках правоохоронних органів. Сучасні технічні засоби дозволяють отримати інформацію без безпосереднього підключення до електронної інформаційної

¹ Говоруха В.І., Степанов В.А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право*. № 3(34). 2020. С. 70–71.

² Кримінальний кодекс України: Верховна Рада України; Кодекс України, Кодекс, Закон від 5 квітня 2001 р. URL: <http://zakon2.rada.gov.ua/laws/show/2341-142>, с. 150.

системи, за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера тощо. Всі ці дії можна вчинити перебуваючи на значній відстані від об'єкта перехоплення. Наприклад, використовуючи спеціальну апаратуру можна «знімати» інформацію з електронної інформаційної системи, розташованої в сусідньому приміщенні, будівлі. Сучасні технічні засоби дозволяють знімати і розшифрувати випромінювання працюючого принтера на відстані до 150 м., а випромінювання моніторів і з'єднувальних кабелів – до 500 м¹.

У протоколі негласної слідчої (розшукової) дії підлягають відображенню такі відомості:

– в пам'яті якого пристрою виявлено віртуальні сліди; -кому належить пристрій; чи має пристрій вихід в мережу Інтернет, інші телекомунікаційні або локальні мережі;

– яка оперативна система функціонує на пристрої (Windows, Linux – на комп'ютері, Windows mobile, Android, Symbianna мобільному телефоні, комунікаторі, планшеті і т.п.);

– в яких файлах виявлені сліди втручання, які саме;

– коли файл був створений, змінений, відкривався востаннє.

Щоб уникнути вивчення кожного файлу комп'ютера (кількість файлів може вимірюватися сотнями тисяч) до проведення негласної слідчої (розшукової) дії необхідно залучати спеціаліста (програміста, системного адміністратора тощо), який може встановити спеціальні фільтри для виявлення інформації, яка може мати відношення до кримінального правопорушення, щодо якого здійснюється досудове розслідування².

Враховуючи функціональні особливості та методи отримання інформації з електронних інформаційних систем, автори виділяють наступні типи СТЗ:

1) засоби для зняття (шляхом фізичного/технічного доступу) інформації з електронних інформаційних систем або з їх частин;

2) спеціалізовані програми для зняття (шляхом програмного проникнення), порушення цілісності, знищення, блокування та/або копіювання інформації з електронних інформаційних систем або з їх частин;

3) закладні пристрої, що розміщують безпосередньо в засобах обчислювальної техніки (USB-портах, системних платах, клавіатурах тощо) або в периферійному обладнанні (модемах, принтерах та інших пристроях)

4) засоби зняття, фіксації та аналізу побічних електромагнітних випромінювань від електронних інформаційних систем;

5) спеціальні засоби для експрес копіювання, руйнування (знищення) інформації з технічних носіїв.

¹ Луцик В. В. Зняття інформації з електронних інформаційних систем. URL: <https://goo.gl/Db2Cnv>, С. 156–157; Олашин М. М., Галяк С.С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем. Вісник Львівського торговельно-економічного університету. Юридичні науки. 2018. Вип. 7. С. 238–239.

² Олашин М. М., Галяк С.С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем. Вісник Львівського торговельно-економічного університету. Юридичні науки. 2018. Вип. 7. С. 239.

Серед інших особливостей застосування таких СТЗ слід виділити:

– подолання системи логічного захисту електронних інформаційних систем;

– пошук, виявлення, обстеження, відбір, фіксація/копіювання інформації;

– передачу інформації третій стороні (при цьому можуть застосовуватись методи кодування чи шифрування інформації, передача за прискореними алгоритмами, активація за розкладом або за допомогою дистанційного керування, використання радіотехнологій);

– інші дії з інформацією в електронних інформаційних системах (порушення цілісності, знищення, блокування).

Як видно із наведених ознак СТЗ, крім зняття інформації з електронних інформаційних систем, такі засоби дозволяють здійснювати інші дії з інформацією, а саме: порушення цілісності, знищення та блокування.

Ці особливості функціонування СТЗ дають підстави для опису дій із отримання доступу до інформації електронних інформаційних систем в контексті пояснення ознаки «отримання інформації»¹.

Зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником.

Верховний Суд колегією суддів Другої судової палати Касаційного кримінального суду встановив, коли зняття інформації з електронних інформаційних систем можливе без дозволу слідчого судді.

Так, у Постанові ВС зазначено, що безпідставним є твердження захисника про те, що під час досудового розслідування було здійснено незаконний (без постанови слідчого судді) доступ до відомостей з електронних інформаційних мереж, який оформлено як протокол огляду предмета – телефона.

Сутність такої негласної слідчої (розшукової) дії, як доступ до зняття інформації з електронних інформаційних систем полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частин, доступ до яких обмежений власником, володільцем або утримувачем системи розміщення її у публічно недоступному місці, житлі чи іншому володінні особи або логічним захистом доступу, а також отримання таких відомостей без відома її власника, володільця або утримувача.

Зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

Що ж стосується інформації, яка була наявна в мобільному телефоні ОСОБА_1, то вона була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем. В даному

¹ Говоруха В.І., Степанов В.А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. Інформація і право. № 3(34). 2020. С. 71–72.

випадку орган досудового розслідування провів огляд предмета – телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону.

За таких обставин Суд не вбачає жодних порушень вимог кримінального процесуального закону при розгляді даного кримінального провадження¹.

5. Установлення місцезнаходження радіоелектронного засобу

Установлення місцезнаходження радіоелектронного засобу є негласною слідчою (розшуковою) дією, яка полягає в застосуванні технічних засобів для локалізації місцезнаходження радіоелектронного засобу, у тому числі мобільного терміналу систем зв'язку, та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження (ч. 1 ст. 268 КПК України).

Проведення цієї негласної слідчої (розшукової) дії забезпечує отримання даних, що сприятимуть оперативному розшуку особи, підозрюваної у причетності до вчинення злочину, за рахунок установлення місцезнаходження персональної радіостанції стільникового радіозв'язку. Проведення цієї негласної слідчої (розшукової) дії забезпечує можливість установлення місцезнаходження у визначений проміжок часу радіоелектронних засобів та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, що належать або використовувались особами, які можуть бути причетними до вчинення злочину, визнані потерпілими або свідками; або поточні координати такого радіоелектронного засобу у просторі й часі².

Безпосереднє установлення місцезнаходження радіоелектронного засобу здійснюється із застосуванням спеціальних технічних засобів та інформаційних технологій. Слідчому доцільно доручати проведення таких дій уповноваженим спеціалістам оперативних підрозділів з залученням оперативно-технічних підрозділів МВС та СБУ України.

Установлення місцезнаходження радіоелектронного засобу частіше за все носить характер дій, спрямованих на підготовку затримання підозрюваного чи провадження інших негласних слідчих (розшукових) дій. Тому застосування такого заходу у невідкладних випадках може здійснюватись до ухвали слідчого судді, яким надається відповідний дозвіл, за правилами ст. 250 КПК України. За умови прийняття рішення слідчого, узгодженого з прокурором, про

¹ Постанова Верховного Суду. 9 квіт. 2020 року. Справа № 727/6578/17. Провадження № 51-4494 км 19. URL: https://reyestr.court.gov.ua/Review/88749345?fbclid=IwAR0gdLCRQGS2SjQNaIuaOMy8VHqgYwxDOVXB_Cnx5kC38LZihxNj8F1rJrA.

² Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1 / О. М. Бандурка, С. М. Блажівський, Е. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація. – Харків: Право, 2012. С. 678.

невідкладність проведення відповідної дії, положення закону про те, що якщо слідчий суддя постановить ухвалу про відмову в наданні дозволу на проведення цієї негласної слідчої (розшукової) дії, то її проведення повинно бути негайно припинено, а отримана внаслідок такої негласної слідчої (розшукової) дії інформація повинна бути знищена (ч. 4 ст. 250 КПК України), фактично носить лише віртуально-попереджувальний характер. В її проведенні на момент ухвали слідчого судді і так, зазвичай, уже не має сенсу, бо мета її встановити місце перебування підозрюваного для його затримання досягнута (затримання здійснено, злочин попереджено).

Рішення про те, що отримана внаслідок такої негласної слідчої (розшукової) дії інформація повинна бути знищена, теж стає формальним, адже сама дія не була спрямована на отримання доказів, а отримана інформація уже втратила актуальність і може бути знищена без проблем для слідства¹.

Установлення місцезнаходження радіоелектронного засобу є без перебільшення одним із найефективніших НСРД та ОРЗ, здатних швидко та якісно вирішувати завдання кримінального провадження і ОРД. Нововведений НСРД характерні всі ознаки негласної роботи та ОРД. Окрім того, вона переважно реалізується оперативними підрозділами. Сутність застосування установлення місцезнаходження радіоелектронного засобу як НСРД чи ОРЗ однакова, різниця полягає лише в організації проведення та правових статусах отриманих результатів. Характерною особливістю установлення місцезнаходження радіоелектронного засобу (НСРД) є те, що її проведення не обмежує конституційні права та свободи людини і громадянина, оскільки об'єктом цієї дії є технічний засіб, а не фізична особа. Крім того, під час установлення місцезнаходження радіоелектронного засобу не контролюється будь-яка інформація, що передається засобами зв'язку, чи інша інформація, якою обмінюються особи, що перебувають у приміщенні, де є радіоелектронний засіб². Для установлення місцезнаходження радіоелектронного засобу отримується лише інформація про взаємне з'єднання телекомунікаційних мереж (інформація про факт спілкування, а не про його зміст, а тому і не може вважатися втручанням у приватне спілкування³. За її результатами (як НСРД) можна встановити факт перебування у певному місці та в певний час конкретної особи, якій належить або в якій є у користуванні радіоелектронний засіб, чи місцезнаходження пристрою⁴.

¹ Установлення місцезнаходження радіоелектронного засобу
https://pidru4niki.com/1497010959159/pravo/ustanovlennya_mistseznahodzhennya_radioelektronnogo_zasobu.

² Федосова О. В. Правові основи застосування негласних слідчих (розшукових) дій при розслідуванні корисливо-насильницьких злочинів. О noua perspectiva a proceselor de integrare europeana a Moldovei si Ucrainei: conferinta inernationala stintsifico-practica, 25–26 martie 2016 / Institutul cercetari juridice si politice al academiilor de stiinta a Moldovei. Chisinau, Republica Moldova : [s. n.]. [Ч. 2]. 2016. P. 222–225

³ Хараберюш О. І. Використання систем мобільного зв'язку щодо протидії контрабанді. *Науковий вісник Херсонського державного університету*. 2014. Вип. 1. Т. 3. С. 209.

⁴ Комарницька О., Прядко В. Установлення місцезнаходження засобу радіоелектронного зв'язку: підготовка та проведення негласної слідчої (розшукової) дії. *Вісник Національної академії прокуратури України*. 2014. № 2 (35). С. 71–78

В ОРД установлення місцезнаходження радіоелектронного засобу найчастіше застосовується для встановлення місця перебування відомої розробленої за оперативно-розшуковою справою (далі – ОРС) особи (фігуранта чи розшукуваного) або для виявлення раніше невідомої особи, шляхом прив'язки до конкретного технічного пристрою із індивідуальними ідентифікуючими ознаками, яка може бути причетною до злочинної діяльності, етапи якої документуються в межах оперативної розробки, до виявлення ознак кримінального правопорушення, яке вчинене або готується; визначення місць, подій, фактів, предметів, речей, пов'язаних із такою особою. Також цей захід інколи використовується як «маяк» для відстеження маршруту переміщення когось або чогось.

Зміст указаного ОРЗ полягає в негласному застосуванні технічних засобів для виявлення місцезнаходження радіоелектронного засобу, зокрема кінцевого обладнання, активованого у мережах операторів рухомого (мобільного) зв'язку без розкриття змісту повідомлень, що передаються, та інших радіовипромінювальних пристроїв. За допомогою отриманої таким способом інформації вирішуються і інші завдання ОРД. У контексті зазначеного, радіоелектронний засіб – це технічний засіб, призначений для передавання та/або приймання радіосигналів радіослужбами (ст.1 Закону України «Про радіочастотний ресурс України»¹. За визначенням окремих дослідників у галузі ОРД, «радіоелектронний засіб – це технічний засіб, що складається з одного або двох передавальних і (або) приймальних пристроїв чи комбінацій таких пристроїв, які мають власні ідентифікаційні ознаки й охоплюють допоміжне обладнання, що призначене для передавання та/або приймання радіосигналів у мережах операторів рухомого (мобільного) зв'язку². Критеріями віднесення до радіоелектронного засобу є також радіовипромінювальні пристрої, активовані у мережах операторів рухомого зв'язку, мобільні телефони, модеми бездротового доступу до мережі інтернет за технологіями GSM, UMTS, HSDPA, WiMAX, LTE тощо та будь-які пристрої, що працюють на основі передавання сигналів завдяки електромагнітним коливанням певної частоти і не належать до телекомунікаційних мереж: радіостанції стаціонарні й портативні (рації), радіомаяки тощо³. Досліджуваний ОРЗ, який за змістом належить до оперативно-технічних заходів (ОТЗ), дає змогу швидко і безпечно виявляти осіб, зокрема і невстановлених, які становлять інтерес для оперативної розробки в межах ОРС. Приміром, у Німеччині (ФРН) одним із методів установлення місцезнаходження радіо-електронного засобу є «контроль радіосоти за допомогою відправки «невидимого СМС»» із використанням комп'ютерної програми «SMS-Blaster» з функцією «Stealth-Ping». Водночас одержувач повідомлення не сповіщається про вхідне СМС, а відправник СМС отримує підтвердження про отримання СМС, з

¹ Про радіочастотний ресурс України : Закон України від 1 червня 2000 р. Офіційний вісник України. 2000. № 26. Ст. 1079.

² Романов В. О. Організація і тактика установлення місцезнаходження радіоелектронного засобу підрозділами Національної поліції України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09. Київ, 2019. С. 7.

³ Кримінальний процес: підручник / Ю.М. Грошевий, В.Я. Тацій, А.Р. Туманянц та ін.; за заг. ред. В.Я. Тація, Ю.М. Грошевого, О.В. Капліної, О.Г. Шило. Харків: Право, 2013. С. 445

якого можна дізнатися, чи включений мобільний апарат підозрюваного. Файл із відповідними даними про зв'язок, зокрема про місцезнаходження мобільного апарату, запитується правоохоронними органами в оператора мобільного зв'язку¹.

6. Право співробітника оперативного підрозділу на ознайомлення та отримання інформації від провайдера телекомунікаційних послуг

Законом України «Про оперативно-розшукову діяльність» надано право співробітнику оперативного підрозділу ознайомлюватися, вивчати, витребувати документи та дані, що характеризують діяльність та спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину тощо, з дозволу слідчого судді в порядку, передбаченому Кримінальним процесуальним кодексом України (ч. 1 ст. 8)².

В даному контексті Вищий спеціалізований суд України зазначає, що оскільки одним із механізмів витребування документів і даних, передбачених КПК України, є процедура тимчасового доступу до речей і документів, передбачена главою 15 КПК України³, оперативні підрозділи мають право звертатися до слідчих суддів суду першої інстанції з клопотаннями про тимчасовий доступ до таких документів згідно з правилами, встановленими статтями 159-166 КПК України, та з урахуванням специфіки суб'єктів оперативно-розшукової діяльності та мети її здійснення (зокрема, змісту та обґрунтування клопотання, додатків до клопотання, підстав для його задоволення тощо). При цьому, слідчому судді слід мати на увазі, що документи і дані, які не характеризують діяльність юридичної особи та спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину чи джерела і розмір їх доходів витребуватися оперативними підрозділами не можуть⁴.

За таких обставин вбачається правильним є подання таких клопотань керівником відповідного оперативного підрозділу або його заступником за погодженням із прокурором. У такому разі клопотання про тимчасовий доступ до документів і відповідна ухвала слідчого судді складаються як нетаємні

¹ Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід : монографія. Харків: Право. 2017. С. 269; Лепеха О. М., Кондратюк О. В. Щодо зміни правового статусу застосування установлення місцезнаходження радіоелектронного засобу. Соціально-правові студії. 2020. Вип. 2 (8). С. 99–100.

² Про оперативно-розшукову діяльність. Закон України від 18.02.1992. № 2135-ХІІ. *Відомості Верховної Ради України*. 1992. № 22. ст. 303.

³ Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Голос України* від 19.05.2012. № 90–91.

⁴ Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні: лист вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 29.01.2013 р. № 223-58/04-13.

документи, без дотримання режиму секретності, оскільки вони не містять відомостей, що становлять державну таємницю (крім випадку, передбаченого п. 9 ч. 1 ст. 162 КПК України)¹.

Поряд з наведеними, відповідно до положень статей 159-164 КПК України, розгляд клопотання про тимчасовий доступ до речей і документів здійснюється за участю особи, у володінні якої знаходяться речі і документи, при цьому неприбуття такої особи без поважних причин або неповідомлення нею про причини неприбуття не є перешкодою для розгляду клопотання².

На перший погляд, наведене роз'яснює питання, пов'язані з отриманням оперативним підрозділом інформації від провайдера телекомунікаційних послуг в межах оперативно-розшукової діяльності. Утім, необхідно пам'ятати, що підготовка клопотання буде здійснюватися в межах ОРД, відповідно таке клопотання може містити відомості, що становлять державну таємницю. Отже, виникає питання, за яких умов може бути присутній представник провайдера телекомунікаційних послуг, якщо він не має допуску до державної таємниці.

Безумовно, положення КПК України передбачають порядок розгляду клопотання слідчим суддею, судом без виклику особи, у володінні якої знаходяться речі чи документи про тимчасовий доступ до яких ставиться питання, якщо стороною кримінального провадження, що звертається із клопотанням, буде доведено наявність передбачених у ч. 2 ст. 163 КПК підстав¹ вважати, що існує реальна загроза зміни або знищення речей чи документів.

Під час дослідження даного питання в наукових джерелах пропонувалося внесення змін до Закону України «Про оперативно-розшукову діяльність», якими передбачити, що дозвіл на надання доступу до такої інформації надається слідчим суддею, який визначено у ст. 247 КПК України, без судового виклику та участі особи, у володінні якого знаходиться інформація³. Тобто, за правилами проведення негласних слідчих (розшукових) дій, на підставі ухвали слідчого судді апеляційного суду. Утім, ознайомлення, вивчення, витребування документів та даних, що характеризують діяльність та спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину не пов'язане з втручанням у приватне спілкування, особисте і сімейне життя особи, які відповідно до Конституції України та КПК України проводяться на підставі рішення слідчого судді апеляційного суду.

Отже, враховуючи наведене, ознайомлення, вивчення, витребування документів та даних, що характеризують діяльність та спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину повинно проводитися на підставі ухвали слідчого судді місцевого суду, за необхідності керівник

¹ Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження (Витяг): Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ від 07.02.2014.

² Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: лист Вищого Спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 № 223-559/0/4-13.

³ Климчук М. П. Тимчасовий доступ до речей і документів як захід забезпечення кримінального провадження. *Юридичний часопис Національної академії внутрішніх справ*. № 2. 2013 С. 188.

оперативного підрозділу обґрунтовує необхідність розгляду такого клопотання без виклику особи, у володінні якої знаходяться відповідні відомості, документи тощо¹.

¹ Тарасенко О.С. Право співробітника оперативного підрозділу на ознайомлення та отримання інформації від провайдера телекомунікаційних послуг. Сучасні проблеми правового, економічного та соціального розвитку держави : тези доповідей VI Міжнародної науково-практичної конференції (Харків, 1 груд 2017 р.). Харків: ХНУВС, 2017. С. 447–449.

Додатки

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

Абонентська лінія зв'язку - лінія телекомунікаційної мережі, яка з'єднує кінцеве обладнання споживача з комутаційною системою та складається з магістральних, розподільних ліній зв'язку і абонентської проводки.

Документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Електронний код (ідентифікатор) кінцевого обладнання - код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо).

З'єднання - установлення зв'язку між кінцевими обладнаннями абонентів для обміну інформацією.

Захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Згода споживача - волевиявлення, виражене споживачем у будь-який спосіб, у тому числі вчинення ним дій, які можуть бути зафіксовані обладнанням оператора, провайдера (голосове, текстове повідомлення, використання сигналів тонового набору тощо).

Зона дії телефонної станції (підстанції) - територія, на якій забезпечується надання послуг споживачам, яким присвоєно телефонний номер такої станції (підстанції).

Зона нумерації - частина території, на якій кінцеві пристрої телефонного зв'язку мають єдиний формат номерів і однаковий код зони.

Ідентифікаційна телекомунікаційна картка - засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо).

Інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Картка попередньо оплаченої послуги - засіб для замовлення та попередньої оплати послуг, що дає право споживачеві на отримання визначеного переліку та/або обсягу послуг оператора, провайдера в межах визначеного активу такого засобу.

Комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Мережевий ідентифікатор споживача - індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в телекомунікаційній мережі чи Інтернеті.

Міжміський телефонний зв'язок - телефонний зв'язок у межах України між споживачами, розташованими в різних зонах нумерації або різних місцевих телефонних мережах.

Міжнародний телефонний зв'язок - телефонний зв'язок із споживачами, розташованими на території інших держав.

Місцева телефонна мережа - телекомунікаційна мережа, яка обмежена територією одного міста, району та забезпечує комутований доступ до інших телекомунікаційних мереж.

Місцевий телефонний зв'язок - телефонний зв'язок між споживачами, розташованими в межах одного міста, району.

Негласні слідчі (розшукові) дії - це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених Кримінальним процесуальним кодексом України (ст. 246 КПК України).

Послуга з доступу до Інтернету - забезпечення можливості з'єднання кінцевого обладнання споживача з Інтернетом.

Послуга з передачі даних - обмін даними між кінцевими обладнаннями абонентів з використанням телекомунікаційних мереж.

Послуги рухомого (мобільного) зв'язку - послуги, які надаються оператором рухомого (мобільного) зв'язку і під час отримання яких кінцеве обладнання абонента може вільно переміщатися в межах телекомунікаційної мережі такого оператора або його роумінг-партнера із збереженням абонентського номера або мережевого ідентифікатора споживача.

Процесуальними документами щодо проведення негласних слідчих (розшукових) дій є постанови, клопотання, доручення, протоколи уповноваженого співробітника (працівника) оперативного підрозділу, слідчого, прокурора, а також ухвали слідчого судді.

Пункт колективного користування - приміщення, де споживачам надаються послуги з використанням розміщених у ньому засобів зв'язку (кінцевого обладнання) оператора, провайдера та/або кінцевого обладнання споживачів (автоматизований переговорний пункт, відділення зв'язку, Інтернет-пункт тощо).

Сеанс зв'язку - процес надання та отримання послуги з моменту встановлення з'єднання до його завершення.

Телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Телефонний зв'язок - вид електрозв'язку для передачі голосових повідомлень у реальному часі з використанням номерного ресурсу телефонної мережі.

Уповноважена особа - співробітник (працівник) уповноваженого оперативного підрозділу, залучений за рішенням керівника до проведення або участі у проведенні негласної слідчої (розшукової) дії, інші особи, залучені за рішенням слідчого, прокурора, оперативного підрозділу.

Уповноважений оперативний підрозділ - оперативний підрозділ, який входить до складу державного органу, визначеного у статті 246 КПК України, залучений за рішенням керівництва органу до здійснення або участі у проведенні негласної слідчої (розшукової) дії.

Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження (витяг щодо тимчасового доступу до речей і документів: <https://zakon.rada.gov.ua/laws/show/n0001740-14#Text>)

Тимчасовий доступ до речей і документів

1) Результати аналізу судової практики свідчать про те, що з клопотаннями про тимчасовий доступ до речей і документів, як правило, звертається сторона кримінального провадження з боку обвинувачення - слідчі та прокурори, в той час як випадки звернення до слідчих суддів з такими клопотаннями сторони кримінального провадження з боку захисту (перш за все, це стосується захисників підозрюваних), є поодинокими, незважаючи на те що закріплення в КПК норми, яка надає стороні кримінального провадження з боку захисту таке право, було спрямоване на впровадження механізму реалізації змагальності сторін та свободи в поданні ними до суду своїх доказів і у доведенні перед судом їх переконливості.

2) КПК, визначаючи порядок та підстави застосування тимчасового доступу до речей і документів, не регламентує строків розгляду клопотання про застосування цього заходу забезпечення кримінального провадження. Обґрунтованою є практика слідчих суддів, які при вирішенні питання про визначення строків розгляду аналізованого клопотання керуються наступним.

Відповідно до ч. 1 ст. 114 КПК для забезпечення виконання сторонами кримінального провадження вимог розумного строку слідчий суддя, суд має право встановлювати процесуальні строки у межах граничного строку, передбаченого цим кодексом, з урахуванням обставин, встановлених під час відповідного кримінального провадження.

Враховуючи закріплення у КПК двох порядків розгляду слідчим суддею, судом клопотання про тимчасовий доступ до речей і документів, встановлювати процесуальні строки їх розгляду доцільно виходячи з наступного:

а) після отримання клопотання про тимчасовий доступ до речей і документів слідчий суддя здійснює судовий виклик особи, у володінні якої знаходяться речі та документи. У такому випадку доцільно призначити клопотання до розгляду у строк, необхідний для отримання особою повістки про судовий виклик;

б) якщо стороною, яка звернулася з клопотанням, доведено наявність достатніх підстав вважати, що існує реальна загроза зміни або знищення речей чи документів, клопотання розглядається слідчим суддею без виклику особи, у володінні якої вони знаходяться. Враховуючи реальну загрозу зміни або знищення речей і документів відповідне клопотання має бути розглянуто невідкладно.

3) Враховуючи необхідність оперативного вирішення питань, які порушуються стороною кримінального провадження в клопотанні про тимчасовий доступ до речей і документів, доцільним є виклик особи, у

володінні якої знаходяться речі чи документи, за допомогою такого способу виклику, передбаченого ч. 1 ст. 135 КПК, який би давав змогу якомога швидше довести до адресата інформацію про місце, час та день розгляду клопотання.

4) Слідчим суддям необхідно враховувати, що оскільки одним із механізмів витребування документів і даних, передбачених КПК, є процедура тимчасового доступу до речей і документів, передбачених главою 15 КПК, оперативні підрозділи мають право звертатися до слідчих суддів суду першої інстанції з клопотанням про тимчасовий доступ до таких документів згідно з правилами, встановленими ст.ст. 159 – 166 КПК, та з урахуванням специфіки суб'єктів оперативно-розшукової діяльності та мети її здійснення (зокрема, змісту та обґрунтування клопотання, додатків до клопотання, підстав для його задоволення тощо). При цьому слідчому судді слід мати на увазі, що документи і дані, які не характеризують діяльність юридичної особи та спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, чи джерела і розмір їх доходів, витребуватися оперативними підрозділами не можуть.

Зважаючи на те, що Законом України «Про оперативно-розшукову діяльність» та КПК не регламентовано процедуру ініціювання відповідного клопотання, на нашу думку, вирішувати це питання доцільно з урахування вимог ч. 6 ст. 9 КПК, при цьому вбачається правильним подання таких клопотань керівником відповідного оперативного підрозділу або його заступником за погодженням з прокурором.

5) Результати аналізу судової практики свідчать про існування випадків недолучення слідчим (прокурором) до клопотання про тимчасовий доступ до речей і документів належним чином засвідченої копії витягу з ЄРДР щодо кримінального провадження, в рамках якого подається клопотання; незазначення в клопотанні правової кваліфікації кримінального правопорушення, а лише вказівка на статтю (частину статті) КК; відсутність повних та конкретних відомостей про речі і документи, тимчасовий доступ до яких планується отримати.

Слідчий суддя Павлоградського міськрайонного суду Дніпропетровської області за участю слідчого СВ Павлоградського МВ ГУМВС України в Дніпропетровській області, розглянувши клопотання про надання тимчасового доступу до речей і документів, відмовив в його задоволенні. Своє рішення слідчий суддя мотивував тим, що в поданому клопотанні слідчий зазначив лише статтю закону України про кримінальну відповідальність, а не правову кваліфікацію кримінального правопорушення при здійсненні досудового розслідування якого порушується питання про тимчасовий доступ до речей і документів.

Окрему проблему становить подання слідчими та прокурорами разом з клопотанням про тимчасовий доступ до речей і документів копій документів, в тому числі витягу з ЄРДР, які належним чином або взагалі не засвідчені, що позбавляє слідчого суддю можливості пересвідчитися в ідентичності цих документів, в той час, як інформація, що в них міститься, має суттєве значення під час розгляду клопотання цієї категорії та може істотно вплинути на висновки слідчого судді.

6) Неоднозначною є практика слідчих суддів при встановленні факту недотримання слідчими та прокурорами вимог кримінального процесуального закону стосовно оформлення клопотання про тимчасовий доступ до речей і документів, оскільки в переважній більшості таких випадків слідчі судді приймають рішення про відмову в задоволенні клопотання або його часткове задоволення. Водночас існує і практика повернення таких клопотань для дооформлення, усунення недоліків тощо.

Слідчий суддя Калінінського районного суду міста Горлівки Донецької області 11.02.2014 повернув для усунення недоліків клопотання слідчого СВ Горлівського МУ ГУМВС України в Донецькій області про тимчасовий доступ до речей і документів у кримінальному провадженні у зв'язку з тим, що у клопотанні некоректно зазначено найменування речей і документів, тимчасовий доступ до яких планується отримати, відсутнє обґрунтування необхідності отримання відомостей, що можуть містити банківську таємницю, а також неправильно зазначено посаду слідчого.

Крім того, мають місце випадки звернення слідчих, прокурорів із клопотаннями про повернення їхніх клопотань для дооформлення.

Слід звертати увагу на те, що на відміну від закріпленого у КПК порядку розгляду клопотання про тимчасове обмеження у користуванні спеціальним правом, відсторонення від посади, арешт майна при регламентації порядку розгляду клопотання про тимчасовий доступ до речей і документів, законодавець не закріпив повноваження слідчого судді повертати таке клопотання у разі його невідповідності встановленим вимогам. Саме тому у подібних випадках необхідно постановляти ухвалу про відмову у задоволенні клопотання, а не про його повернення.

7) Випадки, коли клопотання про надання доступу до речей і документів обґрунтовано лише формально, до нього не додано жодного доказу на обґрунтування викладених слідчим або іншим учасником кримінального провадження, який має право на його подання, доводів, не можуть бути оцінені як недоліки клопотання, оскільки свідчать про їх необґрунтованість.

Враховуючи наведене, не можна оцінити правильною практику слідчого судді, який при розгляді клопотання слідчого про тимчасовий доступ до документів у Ковельському міськрайонному суді Волинської області ухвалою від 15.04.2013 повернув клопотання слідчому для усунення недоліків. У рішенні зазначено, що клопотання належним чином не мотивоване та не наведено доказів, що особа, у володінні якої знаходяться документи, не бажає добровільно передати їх стороні кримінального провадження.

8) Аналіз судової практики свідчить про існування питання про те, яке процесуальне рішення має прийняти слідчий суддя, якщо слідчий органу досудового розслідування, який звернувся з клопотанням про надання дозволу на тимчасовий доступ до речей і документів, не з'явився для розгляду зазначеного клопотання (відмовити у розгляді, відмовити у задоволенні клопотання по суті, призначити розгляд на інший день).

КПК не містить конкретної вказівки слідчому судді на те, яким чином необхідно діяти в разі неявки на розгляд клопотання про тимчасовий доступ до

речей і документів сторони кримінального провадження, якою таке клопотання було подане, враховуючи, що відповідно до ч. 4 ст. 163 КПК клопотання цієї категорії розглядається за участю сторони кримінального провадження.

В такому випадку слідчим суддям необхідно керуватись ч. 5 ст. 163 КПК, відповідно до якої слідчий суддя вправі постановити ухвалу про тимчасовий доступ до речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що мають місце обставини, передбачені п.п. 1, 2, 3 ч. 5 ст. 163 КПК. Неявка без поважної причини сторони кримінального провадження, якою подане клопотання про тимчасовий доступ до речей і документів, свідчить про фактичне не підтримання поданого клопотання та недоведення згаданих обставин, що має оцінюватись як підстава для відмови в задоволенні такого клопотання. Такий підхід слід застосовувати незалежно від того, яка із сторін кримінального провадження (обвинувачення чи захисту) звернулась до слідчого судді із відповідним клопотанням.

Слідчий суддя Заводського районного суду м. Дніпродзержинська Дніпропетровської області, розглянувши клопотання слідчого Заводського РВ Дніпродзержинського МУ УМВС, в задоволенні клопотання про тимчасовий доступ відмовив. Однією з підстав для відмови у задоволенні клопотання стало те, що слідчий не з'явився в судове засідання, хоча був повідомлений належним чином про день, час та місце слухання справи.

9) При зверненні до суду з клопотаннями про тимчасовий доступ до речей і документів слідчими не виконуються вимоги ч. 2 ст. 93 КПК, згідно з якою сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових дій), витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом.

Слідчий суддя Хортицького районного суду м. Запоріжжя відмовив в задоволенні клопотання слідчого про надання доступу до документа форми № 1, що зберігається в СГРФО Комунарського РВ ЗМУ ГУМВС України в Запорізькій області, з метою ознайомитись з документом та зробити його копію. Відмова ґрунтується на тому, що чинне законодавство надає слідчому право одержувати безперешкодно і безоплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості, необхідні у справах про злочин, що знаходяться в провадженні міліції. До того ж, територіальним органом Державної міграційної служби в Запорізькій області є Управління ДМС у Запорізькій області. Отже слідчий просив надати доступ до документів, які знаходяться у володінні органу, якого не існує (СГРФО), що суперечить вимогами п. 4 ч. 1 ст. 164 КПК.

Аналіз судової практики свідчить, що застосуванням заходу забезпечення кримінального провадження органи досудового розслідування намагаються досягти мети, яка саме таким заходам не властива. Зокрема, це стосується випадків, коли у клопотанні порушується питання про тимчасовий доступ до речей і документів з метою збирання доказів.

Клопотання слідчих в окремих випадках ґрунтуються на необхідності правомірного доступу та вилучення речей, які можуть бути речовими доказами. Проте поза увагою слідчого, прокурора, слідчого судді залишається та обставина, що збирання доказів, в тому числі і речових, відбувається через інститут слідчих дій (зокрема, вилучення в ході огляду, проведення обшуку). У таких випадках неправильне розуміння органами досудового розслідування, слідчими суддями положень кримінального процесуального закону фактично зумовлює підміну слідчих дій заходом забезпечення кримінального провадження. Слідчим суддям необхідно враховувати, що згідно з ч. 4 ст. 132 КПК для оцінки потреб досудового розслідування слідчий суддя зобов'язаний врахувати можливість без застосовуваного заходу забезпечення кримінального провадження отримати речі і документи, які можуть бути використані під час судового розгляду для встановлення обставин у кримінальному провадженні. У цьому контексті потрібно враховувати, що речі і документи могли би бути отримані шляхом проведення слідчих дій, тобто без застосування заходів забезпечення кримінального провадження. Крім того, відповідно до ч. 1 ст. 223 КПК саме слідчі (розшукові) дії є діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні.

Слідчий суддя Олександрійського міськрайонного суду Кіровоградської області 13.12.2012 за клопотанням слідчого в кримінальному провадженні за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 121 КК, надав дозвіл на тимчасовий доступ та вилучення речей: ножа - знаряддя злочину, до речі, на який попередньо був накладений арешт, і який знаходиться у голови сільської ради; одягу підозрюваного та померлого потерпілого, які перебувають у фізичних осіб - родичів.

Таким чином, слідчий суддя, погодившись з доводами слідчого та прокурора, мотивував своє рішення тим, що перелічені в клопотанні речі можуть бути речовими доказами, оскільки могли зберегти на собі сліди вчинення кримінального правопорушення.

10) Також слідчі судді іноді відмовляють у задоволенні клопотань про надання тимчасового доступу до документів, які містяться в матеріалах кримінальних справ (проваджень), що перебували в провадженні органів досудового розслідування, з мотивів належності матеріалів кримінального провадження, які перебувають в провадженні органів досудового розслідування, до таємниці досудового розслідування, а тому стороні кримінального провадження ухвалами роз'яснювалась можливість звернення безпосередньо до слідчого чи прокурора щодо надання дозволу до зазначених документів в обсязі, в якому вони визнають за можливе.

11) З іншого боку, одним з проблемних питань правозастосування є питання розгляду клопотань відповідної категорії, в основу яких покладено матеріали оперативно-розшукових справ та інші матеріали, які мають встановлений гриф таємності, оскільки з урахуванням відсутності у слідчих суддів відповідного допуску до роботи з таємними документами, слідчі та прокурори ці матеріали до слідчого судді не подають. З урахуванням

викладеного у слідчих суддів виникають проблеми з розглядом зазначених клопотань, а іноді ці документи є єдиним підтвердженням тих чи інших обставин, на які є посилання в клопотанні, а у зв'язку з цим існують проблеми з прийняттям законного та обґрунтованого рішення про задоволення чи відмову в задоволенні цих клопотань. Таким чином, відсутність допуску до державної таємниці унеможливує оцінку обґрунтованості клопотання про застосування такого заходу забезпечення кримінального провадження.

12) У вимогах до змісту клопотання про тимчасовий доступ до речей і документів (ст. 160 КПК) відсутня вимога про надання інформації про прізвище, ім'я, по батькові фізичної особи або найменування юридичної особи, які мають надати доступ до речей і документів, оскільки на органи досудового розслідування не покладається обов'язок надавати такі відомості, а в ухвалі слідчого судді ці відомості мають бути обов'язково зазначені (ст. 164 КПК).

При надходженні клопотань, у яких відсутня інформація про прізвище, ім'я, по батькові фізичної особи або найменування юридичної особи, слід керуватись наступним. Відповідно до п. 4 ч. 2 ст. 160 КПК у клопотанні про тимчасовий доступ до речей і документів повинні бути зазначені підстави вважати, що речі і документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи. Згідно з п. 1 ч. 5 ст. 163 КПК, слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність підстав вважати, що ці речі або документи перебувають чи можуть перебувати у володінні відповідної фізичної або юридичної особи. Крім того, при вирішенні цього питання слід враховувати, що ч. 1 ст. 163 КПК передбачено обов'язок слідчого судді здійснити судовий виклик такої особи, а тому слід визнати правильною практику слідчих суддів, які вимагають від слідчого або іншого учасника кримінального провадження, який звернувся із клопотанням, обов'язкового викладення цих відомостей у клопотанні, посилаючись на згадані норми закону, а у протилежному випадку - відмовляють у задоволенні таких клопотань, оскільки по суті без зазначення особи, яка має надати доступ до речей та документів, клопотання не може бути визнано обґрунтованим.

13) Водночас слід звернути увагу на те, що відповідно до п. 1 ч. 1 ст. 164 КПК в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів має бути зазначено прізвище, ім'я та по батькові особи, якій надається право тимчасового доступу до речей і документів. Проте із аналізу судової практики вбачається, що існують випадки ігнорування цієї вимоги, оскільки у відповідних ухвалах зазначаються лише ініціали особи.

14) Причиною відмови у задоволенні зазначених клопотань було те, що слідчі (прокурор) просили надати тимчасовий доступ до речей і документів, які знаходяться у володінні філій (філій операторів, банків, фірм), однак це суперечить вимогам п. 4 ч. 2 ст. 160 КПК, оскільки філія не має статусу юридичної особи у розумінні цієї норми законодавства, а тому надання тимчасового доступу до речей і документів, які знаходяться у володінні такої філії є неможливим.

15) Результати аналізу судової практики свідчать про те, що слідчими ігнорується не лише наведена законодавча вимога, але й необґрунтовано зазначається у клопотаннях про їх розгляд без участі осіб, у володінні яких перебувають певні речі або документи. Клопотання містять формальні посилання на можливість знищення особами речей та документів, однак вони жодним чином не підтверджені будь-якими доказами.

Зазначений факт необґрунтованості клопотань в частині його розгляду без участі особи не завжди береться до уваги слідчими суддями, що призводить до безпідставного схвалення позиції слідчого або прокурора про такий порядок його розгляду.

До Михайлівського районного суду Запорізької області 26.12.2012 надійшло клопотання про тимчасовий доступ до речей і документів у кримінальному провадженні за ознаками злочину, передбаченого ч. 1 ст. 382 КК – про надання тимчасового доступу та можливість вилучення виконавчого провадження про стягнення з ФГ "В." на користь В. 49967 грн. Отримавши клопотання, слідчий суддя того ж дня розглянув його, не повідомивши особу, у володінні якої знаходяться документи, і не мотивувавши свого рішення про можливість розгляду клопотання без участі представника ВДВС Михайлівського РЮО.

16) Мотивуючи ухвалу про відмову в задоволенні клопотання, слідчі судді формально вказують на те, що слідчий не довів значення речей і документів для встановлення обставин у кримінальному провадженні.

Слід акцентувати увагу слідчих суддів, що лише у випадку подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, зазначається про неможливість іншим способом довести обставини, які передбачаються довести за допомогою цих речей і документів. За таких обставин вимога слідчих суддів до осіб, які звертаються із клопотанням про тимчасовий доступ до речей і документів, доводити, що іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів, неможливо, є неправомірною.

17) В багатьох випадках формальністю та неналежною обґрунтованістю характеризуються клопотання про тимчасовий доступ до речей і документів, в яких порушується питання про їх вилучення. Органи досудового розслідування порушують питання про вилучення речей і документів при зверненні до слідчих суддів з відповідними клопотаннями, належним чином не обґрунтовуючи необхідність вилучення речей, а в більшості випадків це стосується вилучення оригіналів документів, без зазначення підстав, з яких для досягнення цілей кримінального провадження неможливо обмежитись вилученням належним чином засвідчених копій таких документів.

18) У цьому контексті слід враховувати і те, що відповідно до ч. 7 ст. 163 КПК, слідчий суддя, суд в ухвалі про тимчасовий доступ до речей і документів може дати розпорядження про надання можливості вилучення речей і документів, якщо сторона кримінального провадження доведе наявність достатніх підстав вважати, що без такого вилучення існує реальна загроза зміни

або знищення речей чи документів або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів.

Водночас результати аналізу судової практики свідчать про існування випадків, коли слідчі судді вказують на необхідність подання стороною кримінального провадження окремого клопотання про надання дозволу на вилучення документів. Така вимога слідчих суддів не ґрунтується на положеннях КПК.

19) Згідно зі ст. 162 КПК передбачено спеціальний порядок доступу до інших видів охоронюваних законом таємниць, а саме: отримання судового дозволу на підставі вмотивованого клопотання про тимчасовий доступ до речей та документів. Наприклад, комерційна та банківська таємниця, особисте листування, персональні дані про особу та інше. У зв'язку з можливістю такого широкого доступу до інформації про особу на практиці інколи виникає проблема меж співвідношення процесуальної дії тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, та можливості проведення певних видів негласних слідчих (розшукових) дій.

Під час здійснення судового контролю за дотриманням прав, свобод та законних інтересів осіб у кримінальному провадженні слідчим суддям необхідно враховувати, що у КПК передбачено декілька процесуальних дій, які мають певну схожість. Зокрема, у ст. 159 та п. 7 ч. 1 ст. 162 КПК передбачено такий захід забезпечення кримінального провадження, як тимчасовий доступ до документів, які знаходяться в операторів та провайдерів телекомунікацій та містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання, а ст.ст. 263 та 268 КПК передбачено такі негласні слідчі (розшукові) дії, як зняття інформації з транспортних телекомунікаційних мереж та установлення місцезнаходження радіоелектронного засобу відповідно. Зазначені процесуальні дії слід відмежовувати таким чином:

дії, передбачені ст.ст. 263 та 268 КПК, є негласними слідчими (розшуковими) діями, дозвіл на проведення яких надає слідчий суддя суду апеляційної інстанції. Інформація щодо цих дій згідно із Законом України «Про державну таємницю» та п.п. 4.12.4 і 4.12.5 Зводу відомостей, що становлять державну таємницю, затвердженого наказом Служби безпеки України від 12.08.2005 № 440, містить відомості, що становлять державну таємницю. Водночас дії, передбачені ст. 159, п. 7 ч. 1 ст. 162 КПК, є заходами забезпечення кримінального провадження, дозвіл на застосування яких надає слідчий суддя суду першої інстанції, при цьому відомості щодо таких дій не становлять державної таємниці;

тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання тощо і не дають можливості втрутитися у приватне спілкування, тобто отримати доступ до змісту інформації, що передається. А зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК) є

різновидом втручання у приватне спілкування, оскільки здійснюється доступ до змісту повідомлень будь-якого виду та інформації, що передається особою під час зв'язку;

у ст.ст. 159, 162 КПК передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), у тому числі про місцезнаходження радіоелектронного засобу у певний день та час. Водночас визначена у ст. 268 КПК негласна слідча (розшукова) дія - установлення місцезнаходження радіоелектронного засобу - передбачає локалізацію (моніторинг) місцезнаходження радіоелектронного засобу в режимі реального часу (тобто дає змогу отримати інформацію про те, де перебуває відповідний засіб на момент спостереження за ним, визначити маршрут його перебування).

Враховуючи наведене, слідчі судді обґрунтовано відмовляють у задоволенні клопотань і при цьому зазначають, що орган досудового розслідування звернувся з клопотанням, яке підлягає розгляду слідчими суддями апеляційного суду, оскільки вимоги, які зазначаються у цих клопотаннях, стосуються фактично негласних слідчих (розшукових) дій, зокрема, встановлення місцезнаходження радіоелектронного засобу, втручання в приватне спілкування, оскільки в клопотанні ставиться питання про надання інформації щодо невідомого кола осіб.

20) Поодинокими при розгляді аналізованого виду заходу забезпечення кримінального провадження є випадки повторних звернень із клопотаннями про тимчасовий доступ до речей і документів, коли ухвала слідчого судді у визначений в ній строк не була виконана, як з об'єктивних причин, так і безпідставно. Заборони на звернення із повторним клопотанням КПК не встановлює, як і не встановлює обов'язку слідчого судді відмовити у задоволенні повторного клопотання. Враховуючи наведене, факти попереднього звернення із аналогічним клопотанням та невиконання ухвали, прийнятої за результатами розгляду такого клопотання, не мають правового значення при розгляді повторного клопотання.

21) Ухвала про тимчасовий доступ до речей і документів має відповідати вимогам ст. 164 КПК. Доцільним є зазначення у відповідній ухвалі, що у разі невиконання ухвали про тимчасовий доступ до речей і документів, слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів, має право постановити ухвалу про проведення обшуку з метою відшукування та вилучення зазначених речей і документів.

22) Результати аналізу судової практики свідчать про існування ухвал слідчих суддів, в резолютивних частинах яких відсутнє роз'яснення відповідно до ст. 166 КПК наслідків невиконання ухвали слідчого судді про тимчасовий доступ до речей і документів, не зазначений перелік документів з їх назвою, описом, іншими відомостями, які дають можливість визначити речі і документи, до яких наданий тимчасовий доступ, взагалі відсутня вказівка про строк дії ухвали.

06.06.2013 слідчий суддя Гуляйпільського районного суду Запорізької області, розглянувши клопотання слідчого СВ Гуляйпільського РВ ГУМВС

України в Запорізькій області про надання тимчасового доступу до речей підозрюваного ОСОБА_1, в резолютивній частині ухвали не зазначив що може бути наслідком її невиконання.

23) Усупереч вимогам КПК слідчі судді за результатами розгляду окремих клопотань зобов'язують володільців документів виготовляти їх копії.

24) Ухвали слідчих суддів за результатами розгляду клопотання про тимчасовий доступ до речей і документів не підлягають оскарженню в апеляційному порядку, крім ухвал про задоволення клопотання про тимчасовий доступ до речей і документів, які посвідчують користування правом на здійснення підприємницької діяльності, або інших, за відсутності яких особа - підприємець чи юридична особа позбавляються можливості здійснювати свою діяльність.

В порушення вимог ч. 3 ст. 309 КПК в ухвалях деяких слідчих суддів є посилання на можливість оскарження ухвали в апеляційному порядку.

Список використаних джерел

1. Бабкова В. С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України*. 2018. № 2 (37). С. 70–71.
2. Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід: монографія. Харків: Право. 2017. 376 с.
3. Бем М. Отримання доступу до речей і документів у світлі практики ЄСПЛ. URL: <https://vkr.ua/publication/otrimannya-dostupu-do-rechey-i-dokumentiv-u-svitli-praktiki-iespl>.
4. Герасимчук А. Я. Зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України). *Адвокат*. URL: <https://www.facebook.com/advocate.mariupol/posts/269639480037047>.
5. Говоруха В. І., Степанов В. А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право*. № 3(34). 2020. С. 71–72.
6. Звіт за результатами аналізу ринку послуг з надання у користування каналів електров'язку зі швидкістю до 2 Мбіт/с кінцевим споживачам. Додаток до рішення НКРЗІ від 26.10.2021 р. № 403.
7. Климчук М. П. Тимчасовий доступ до речей і документів як захід забезпечення кримінального провадження. *Юридичний часопис Національної академії внутрішніх справ*. № 2. 2013 с. 185-189, с. 188.
8. Комарницька О., Прядко В. Установлення місцезнаходження засобу радіоелектронного зв'язку: підготовка та проведення негласної слідчої (розшукової) дії. *Вісник Національної академії прокуратури України*. 2014. № 2 (35). С. 71–78
9. Кримінальний процес: підручник / Ю.М. Грошевий, В.Я. Тацій, А.Р. Туманянц та ін.; за заг. ред. В.Я. Тація, Ю.М. Грошевого, О.В. Капліної, О.Г. Шило. Харків: Право, 2013. 824 с.
10. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Голос України* від 19.05.2012. № 90–91.
11. Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1 / О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація. – Харків: Право, 2012. 768 с.
12. Кузубова Т. О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в Україні. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 117–123.
13. Лепеха О. М., Кондратюк О. В. Щодо зміни правового статусу застосування установлення місцезнаходження радіоелектронного засобу. *Соціально-правові студії*. 2020. Вип. 2 (8). С. 99–100.
14. Луцик В. В. Зняття інформації з електронних інформаційних систем. URL: <https://goo.gl/Db2Cnv>, с. 156–157.
15. Михайленко В., Островська О. Питання тимчасового доступу до вмісту електронної поштової скриньки. URL: [47](https://yur-</div><div data-bbox=)

gazeta.com/publications/practice/inshe/pitannya-timchasovogo-dostupu-do-vmistuelektronnoyi-poshtovoyi-skrinki.html.

16. Олашин М. М., Гапак С.С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем. *Вісник Львівського торговельно-економічного університету. Юридичні науки*. 2018. Вип. 7. С. 238–239.

17. Особливості проведення негласних слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень. URL: <https://sa.dn.ua/osoblivosti-provedennya-neglasnikh-sl/3/>

18. Постанова Верховного Суду від 9 квіт. 2020 року. Справа № 727/6578/17. Провадження № 51-4494 км 19. URL: https://reyestr.court.gov.ua/Review/88749345?fbclid=IwAR0gdLCRQGS2SjQNALuaOMy8VHgqYwxDOVXB_Cnx5kC38lZihxNj8F1gJrA.

19. Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: лист Вишого Спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 № 223-559/0/4-13.

20. Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні: лист Вишого Спеціалізованого суду України з розгляду цивільних і кримінальних справ від 29.01.2013 р. № 223-58/04-13.

21. Про оперативно-розшукову діяльність. Закон України від 18.02.1992. № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. ст. 303.

22. Про радіочастотний ресурс України : Закон України від 1 червня 2000 р. Офіційний вісник України. 2000. № 26. Ст. 1079.

23. Романов В. О. Організація і тактика установаження місцезнаходження радіоелектронного засобу підрозділами Національної поліції України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09. Київ, 2019. 20 с.

24. Тарасенко О.С. Право співробітника оперативного підрозділу на ознайомлення та отримання інформації від провайдера телекомунікаційних послуг. *Сучасні проблеми правового, економічного та соціального розвитку держави*: матеріали VI Міжнар. наук.-практ. конф. (Харків, 1 груд 2017 р.). Харків: ХНУВС, 2017. С. 447–449.

25. Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження (Витяг): Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ від 07.02.2014.

26. Установлення місцезнаходження радіоелектронного засобу https://pidru4niki.com/1497010959159/pravo/ustanovlennya_mistseznahodzhennya_radioelektronnoho_zasobu.

27. Ухвала Київського апеляційного суду від 16 берез. 2021 року. URL: <https://vkursi.pro/vsudi/decision/95595884>.

28. Ухвала Октябрського районного суду м. Полтави від 17.01.2019 р. у справі № 554/1862/18. Провадження №1-кц/554/1132/2019. *Єдиний державний*

реєстр судових рішень. URL: <https://youcontrol.com.ua/ru/catalog/court-document/79267173/>

29. Федосова О. В. Правові основи застосування негласних слідчих (розшукових) дій при розслідуванні корисливо-насильницьких злочинів. О noua perspectiva a proceselor de integrare europeana a Moldovei si Ucrainei: conferinta internationala stiintifico-practica, 25–26 martie 2016 / Institutul cercetari juridice si politice al academiilor de stiinta a Moldovei. Chisinau, Republica Moldova: [s. n.]. [Ч. 2]. 2016. Р. 222–225

30. Хараберюш О. І. Використання систем мобільного зв'язку щодо протидії контрабанді. *Науковий вісник Херсонського державного університету*. 2014. Вип. 1. Т. 3. С. 208–211.

Наукове видання

ТАРАН Олена Вікторівна
БРИСКОВСЬКА Оксана Миколаївна
ТАРАСЕНКО Олег Сергійович
ВОЗНЮК Андрій Андрійович та ін.

**ВИКОРИСТАННЯ ІНФОРМАЦІЇ, ЩО ЗНАХОДИТЬСЯ В
ОПЕРАТОРІВ ТА ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ У
КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ**

Методичні рекомендації

Комп'ютерна верстка О. М. Брисковська

Підписано до друку 16.12.2021. Формат 60x84/16.
Папір офсетний. Ум. друк. арк. 3,02.
Тираж 50 прим.

Віддруковано в друкарні ТОВ «7БЦ»
03087, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017