Садіг ТАГІЄВ,
голова Апеляційного суду Чернігівської області,
кандидат юридичних наук

ТИМЧАСОВИЙ ДОСТУП ДО ІНФОРМАЦІЇ, ЯКА ЗНАХОДИТЬСЯ В ОПЕРАТОРІВ І ПРОВАЙДЕРІВ ТЕЛЕКОМУНІКАЦІЙ, У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Новим Кримінальним процесуальним кодексом (КПК) України був запроваджений інститут слідчих суддів у судах першої та апеляційної інстанцій (пункт 18 ч. 1 ст. 3 КПК). Якщо слідчі судді апеляційного суду здійснюють судовий контроль при проведенні негласних (розшукових) слідчих дій, передбачених главою 21 КПК, то до компетенції слідчих суддів місцевих судів віднесено здійснення контролю при проведенні численних слідчих дій, у тому числі при тимчасовому доступі до речей і документів (глава 15 КПК).

Враховуючи, що телекомунікаційні технології дуже швидко розвиваються, і зараз вже важко уявити життя сучасної людини без мобільного телефону, електронної пошти, контактів у соціальних мережах тощо, природно, що телекомунікаційні технології все частіше використовуються як при вчиненні кримінальних правопорушень, так і при їх розкритті.

Через комплексно-програмні пристрої операторів і провайдерів телекомунікаційних мереж (далі – ОіПТ) проходить потік інформації, частина якої залишається в пам'яті для технологічних цілей (статична інформація), а інша частина проходить як «наскрізна» і є інформацією динамічною, яка може бути перехоплена лише на підставі ухвали слідчого судді апеляційного суду. Водночас до статичної інформації тимчасовий доступ можливий на підставі ухвали слідчого судді місцевого суду після розгляду клопотання прокурора або слідчого.

Метою статті є висвітлення проблемних питань судового контролю при розмежуванні статичної та динамічної інформації, що знаходиться в ОіПТ, визначення, до якої її категорії і в якому обсязі можливий тимчасовий доступ, а також забезпечення правильного його процесуального оформлення з метою дотримання конституційних прав людини на недоторканність кореспонденції та телефонних розмов.

Дослідженню різних аспектів забезпечення права особи на недоторканність житла приділено значну увагу в науковій літературі, зокрема у працях О. Биваліна, О. Бикова, В. Бойко, В. Бринцева, Л. Воєводіна, Л. Головко, І. Гришина, Ю. Грошевого, В. Коновалової, В. Маляренка, А. Олійника, І. Петрухіна, П. Пилипчука, Ф. Рудинського, В. Шелестюкова, В. Шепитька, В. Чернобука та інших правознавців.

У сучасному суспільстві, коли спостерігається бурхливе зростання засобів і способів міжособистісного спілкування, з'являються нові інформаційні технології, формується єдина багаторівнева база персональних даних, втілюються у життя ідеї будівництва «електронної держави», тобто в умовах так званої технічної трансформації українського суспільства найбільш гостро постає правова проблема створення дієвого механізму, який би забезпечував недоторканність сфери приватного життя кожної людини, що гарантує таємницю індивідуальних повідомлень, переданих за допомогою телекомунікаційних мереж і без таких.

Стрімке зростання інформаційної інфраструктури в усьому світі і, зокрема, в Україні на початку XXI ст. призвело до необхідності по-іншому поглянути на правову природу і способи захисту одного з базових інститутів міжнародного та вітчизняного законодавства – права на недоторканність приватного життя, складовою якого є закріплене в ст. 31 Конституції України право кожного на таємницю листування, телефонних переговорів, телеграфної та інших видів кореспонденції.

Разом із забезпеченням права на недоторканність приватного життя актуальним стає питання встановлення обмежень цього права пропорційно цінностям, які захищаються Конституцією та міжнародно-правовими актами. Чинне національне законодавство закріплює легітимні обмеження, що враховують співмірність інтересів людини, суспільства і держави, а межі обмежень не повинні довільно визначатися правозастосовними, в тому числі правоохоронними, органами.

Загострення криміногенної обстановки, зростання рівня злочинності, зрощення її з державним апаратом, підвищення технічної оснащеності злочинців, ускладнення способів зв'язку між ними, використання сучасного радіозв'язку, застосування новітніх інформаційних технологій, можливостей Інтернету та інші негативні чинники, – все це, безумовно, ускладнює і без того непросту діяльність правоохоронних органів зі своєчасного та якісного розкриття і розслідування злочинів. «Технізація» злочинності, оснащення злочинних угруповань сучасними засобами комунікації – від мобільних стільникових телефонів до засобів космічного зв'язку – і широке їх використання під час вчинення різноманітних акцій поставили питання про вжиття

правоохоронними органами адекватних заходів, що дають змогу оперативно запобігати злочинам і розкривати їх[1].

Водночас слід пам'ятати, що можливість отримання та використання інформації, яка є у операторів мобільного зв'язку, пов'язана з тимчасовим обмеженням деяких конституційних прав, передбачених ст.ст. 30, 31, 32 Конституції України[2].

Підстави і порядок здійснення заходів, пов'язаних із тимчасовим обмеженням конституційних прав і свобод людини і громадянина, визначені новим КПК України, законами України від 18 лютого 1992 р. «Про оперативно-розшукову діяльність», від 20 грудня 1990 р. «Про міліцію», від 26 грудня 2002 р. «Про контррозвідувальну діяльність», від 30 червня 1993 р. «Про організаційно-правові основи боротьби з організованою злочинністю», постановою Пленуму Верховного Суду України від 28 березня 2008 р. № 2 «Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства». Також у Законі України від 18 листопада 2003 р. «Про телекомунікації» визначаються відповідні терміни (ст. 1), встановлюється правова основа діяльності у галузі телекомунікації, закріплюються повноваження держави щодо регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у цій діяльності або користуються телекомунікаційними послугами.

Верховенство права, зокрема, передбачає, що втручання органів виконавчої влади у права осіб має підлягати ефективному контролю, який зазвичай має здійснюватись судовим органом, оскільки судовий контроль надає найбільші гарантії незалежності, безсторонності та здійснення належного провадження[3].

На сьогодні діяльність суду під час проведення дізнання і досудового слідства в науковій літературі розглядається, як правило, через здійснення функції судового контролю[4].

Повноваження суду реалізуються ним під час вирішення подань органів досудового розслідування про обмеження конституційних прав та свобод особи, а також під час розгляду скарг на дії слідчого та прокурора. Однак власне термін «судовий контроль» не тлумачиться жодним законодавчим актом. Як слушно зазначає В. Лазарєва, питання про правильне визначення назви

---

[1] Див.: Криминалистнка: Учебн. / Под ред. *Р.С. Белкина*. – М.: Издательская группа «Норма-Инфра-М», 2000. – С. 687.

[2] Відомості Верховної Ради України – 1996. – № 30. – Ст. 141.

[3] Див.: Пункт 55 рішення Європейського суду з прав людини у справі «Klass and Others v. Germany».

[4] Див.: *Брынцев В.Д.* Судебная власть (правосудие). Итоги реформ 1992–2003 гг. на Украине. – Харьков, 2001. – 224 с.; *Маляренко В.Т.*, *Пилипчук П.П.* Межі судового контролю за додержанням прав і свобод людини в стадії попереднього розслідування кримінальної справи // Право України. – 2001. – № 4. – С. 40.

судової діяльності на стадії досудового слідства має принциповий характер, оскільки помилкова позиція може призвести до покладення на суд обов'язку, який є ідентичним прокурорському нагляду, тобто внаслідок цього суд певною мірою стає відповідальним за допущені органами розслідування порушення прав і свобод людини і громадянина[1].

Як зазначалось, більшість вчених-процесуалістів визначають діяльність суду на стадії досудового розслідування як «судовий контроль». Так, Ю. Грошевий та І. Марочкін розглядають контрольну функцію суду як контроль за законністю і обґрунтованістю рішень і дій державних органів і посадових осіб, суть якого полягає у тому, що заінтересовані у справі особи можуть оскаржити в суді певні процесуальні рішення[2]. А. Туманянц визначає судовий контроль (контрольну функцію суду в кримінальному судочинстві) як захист прав громадян шляхом контролю та перевірки застосування заходів примусу, пов'язаних з обмеженням цих прав[3].

Вчені, як правило, виокремлюють 2 види судового контролю: попередній (дозвільний) та подальший. Д. Філін вважає, що суд на досудових стадіях кримінального процесу виконує 2 функції: судового контролю (подальшого) та забезпечення законності обмеження конституційних прав громадян[4].

Ще одна точка зору полягає у тому, що суд на стадії досудового розслідування виконує функцію захисту прав і свобод людини і громадянина[5]. Існує також думка, відповідно до якої «судовий контроль» не може бути самостійною функцією судової влади в кримінальному судочинстві, оскільки така діяльність є управлінською та здійснюється лише органами управління і контролю щодо підпорядкованих та підконтрольних структур[6]. Як зазначає В. Півненко, передбачені Конституцією України рішення, які приймаються судами у кримінальному судочинстві на його досудових стадіях, не можна віднести до категорії «контрольних», оскільки в усіх цих випадках істотне обмеження конституційних прав і свобод людини здійснюється безпосередньо суддею на одностороннє прохання слідчого і прокурора[7].

Водночас оцінка суддею обґрунтованості проведення слідчої дії, про яку у своєму поданні клопоче слідчий, потребує особливої виваженості, ретельного врахування значного обсягу інформації, частина якої має вірогідний ха-

---

[1] Див.: *Лазарева В.А.* Теория и практика судебной защиты в уголовном процессе. – Самара, 2000. – С. 71.

[2] Див.: *Грошевий Ю.М., Марочкін І.С.* Органи судової влади в Україні. – К., 1997. – С. 7.

[3] Див.: *Туманянц А.Р.* Контрольні функції суду у сфері кримінального судочинства. – Харків, 2000. – С. 19–20.

[4] Див.: *Філін Д.* Функції суду в досудових стадіях кримінального процесу // Право України. – 2005. – № 1. – С. 64–65.

[5] Див.: *Лазарева В.А.* Судебная власть и уголовное судопроизводство // Государство и право. – 2001. – № 5. – С. 51.

[6] Див.: *Півненко В.* Судовий контроль. Чи може він бути самостійною функцією органів судової влади в кримінальному судочинстві // Прокуратура. Людина. Держава. – 2004. – № 3. – С. 104–105.

[7] Див.: *Півненко В.* Вказ. праця. – С. 107.

рактер, а також обстановки, в якій діє слідчий на певному етапі розслідування[1]. Від правильного встановлення судом наявності підстав для проведення певних слідчих дій часто залежить результат вирішення справи.

У рамках здійснюваної судової реформи у прийнятому новому КПК України законодавець передбачив процесуальну можливість тимчасового доступу до інформації, яка знаходиться у ОіПТ, про зв'язок абонента, надання послуг тощо (пункт 7 ст. 162, пункт 6 ст. 163 КПК України) як захід забезпечення кримінального провадження. Ця інформація віднесена до охоронюваної законом таємниці, яка міститься в речах і документах (глава 15 КПК).

У ч. 1 ст. 1 Закону «Про телекомунікації» визначаються відповідні терміни:

телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж, мереж мобільного та звичайного (цифрового) телефонного зв'язку;

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, Інтернет-мереж.

Передбачена також можливість зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК) та установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК) як негласна слідча (розшукова) дія.

У зв'язку з прийняттям нового КПК України виникає багато питань, пов'язаних з розглядом клопотань про зняття інформації з каналів телекомунікаційних мереж та розмежуванням повноважень апеляційного суду та місцевих судів щодо розгляду цих клопотань.

Необхідно зауважити, що інформація, яка надходить в телекомунікаційні мережі, поділяється на динамічну та статичну.

Динамічна – це інформація «наскрізна», яка передається через мережу та не фіксується, не зберігається в пам'яті програмно-комплексного обладнання ОіПТ (наприклад, зміст розмов).

Проте відповідно до ч. 4 ст. 39 Закону «Про телекомунікації» ОіПТ зобов'язані власним коштом встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і

[1] Див.: *Чорнобук В.І.* Законність та обґрунтованість процесуальних рішень судді в порядку судового контролю у судових стадіях кримінального процесу: Автореф. дис. … канд. юрид. наук. – Одеса, 2007. – С. 10.

тактичних прийомів їх проведення. ОіПТ зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу. Було б доцільним змінити цю норму Закону, додавши після слів «оперативно-розшукових» слово «слідчих».

Таким чином, динамічна інформація у ОіПТ без наявності потреби не зберігається.

Статична – це інформація про споживача та про телекомунікаційні послуги, яка на відміну від динамічної знаходиться (накопичується, змінюється та знищується) у ОіПТ протягом певного часу.

Інформація про споживача та про телекомунікаційні послуги, що їх він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача (ч. 3 ст. 34 Закону «Про телекомунікації»).

Найчастіше при розслідуванні кримінальних правопорушень з'являється інтерес у таких даних, які зберігаються у ОіПТ:

• факт отримання послуг, їхня тривалість, зміст, маршрути передавання тощо;

• за відомим номером абонента встановлення IMEI-коду терміналу (мобільного телефону, інших пристроїв) або IMEI-кодів всіх терміналів, якими користувався відповідний абонент у зазначений період часу;

• за відомим IMEI-кодом терміналу встановлення номера абонента або всіх номерів абонентів, які користувалися цим терміналом у зазначений період часу;

• вибірка вхідних/вихідних дзвінків, SMS, MMS та інших повідомлень конкретного абонента у зазначений період часу;

• встановлення місця перебування (в межах соти) конкретного терміналу з прив'язкою до часу, категорії самих станцій, порядку естафетної передачі, режиму роумінгу тощо;

• встановлення номерів ваучерів поповнення балансу абонента з метою встановлення місця придбання;

• вибірка всіх активних терміналів, які знаходилися в певному квадраті місцевості у певний час;

• встановлення номера абонента користувача Інтернету за допомогою мобільного терміналу за протоколом GPRS/EDGE/CDMA в разі, якщо відома його IP-адреса і час виходу в Інтернет під нею;

• постановка на облік певного номера абонента або IMEI-номера терміналу з подальшим повідомленням замовника у разі появи вказаних абонентів або терміналів в мережі (таймер відсутності);

• характеристика та індекс закритих груп користувачів.

Крім цього, в мережі Інтернет у провайдерів зберігаються такі дані, які можуть становити інтерес для слідства:

• хостинг – розміщення інформації на сервері, що постійно знаходиться у мережі;

• адреса електронної пошти (e-mail) – сховище, де зберігаються копії відправлених листів (поштова скринька);

• спам – інформація, отримана поза бажанням або всупереч бажанню власника електронної пошти;

• UIN – універсальний ідентифікаційний номер у парі з паролем конкретної особи для ICQ – служби миттєвого обміну повідомленнями в мережі Інтернет;

• сайт – місце у мережі Інтернет, сукупність електронних документів (файлів) особи (фізичної або юридичної) у мережі, що об'єднані під одними ім'ям або IP-адресою;

• доменне ім'я – імена різних рівнів напрямів (наприклад, ua.svoboda.org.);

• IP-адреса – мережева адреса вузла у мережі (позначається числами, наприклад 192.186.5.112);

• Skype – програмне забезпечення з закритим кодом, що забезпечує цифровий голосовий та відеозв'язок (зберігаються облікові записи користувачів і резервні копії списків їх контактів).

Слід зазначити, що це – не вичерпна статична інформація, яка знаходиться в ОіПТ.

Далі слід звернути увагу на значення та тлумачення слів, зазначених у пункті 7 ст. 162 КПК України: «...інформація, яка знаходиться...», та у ч. 1 ст. 263 КПК України: «...забезпечують передавання інформації...», які розмежовують компетенцію слідчого судді місцевого суду та слідчого судді апеляційного суду. Відповідно, слідчі судді місцевих судів уповноважені розглядати клопотання про тимчасовий доступ до статичної інформації, яка знаходиться у ОіПТ, тобто до інформації про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміну, маршрути передавання тощо (пункт 7 ст. 162 КПК України). Слідчі судді апеляційних судів у свою чергу розглядають клопотання про зняття динамічної інформації, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків, повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу (ч. 1 ст. 263 КПК України).

Інформація, яка зосереджена в пам'яті комплексно-програмного устаткування ОіПТ, накопичується і використовується для модернізації, оптимізації, контролю техніко-економічних показників та задоволення інформаційних послуг споживачів, тобто використовується ними для забезпечення технологічних процесів у мережі. Так, згідно з пунктом 7 ч. 1 ст. 39 Закону «Про телекомунікації» ОіПТ зобов'язані зберігати записи про надані телекомунікаційні послуги протягом строку позовної давності, визначеного законом, та надавати інформацію про надані телекомунікаційні послуги в порядку, встановленому законом.

За допомогою додаткових програмно-апаратних комплексів, встановлених на площадці оператора, можлива постановка на відстеження зразку голосу конкретної особи із встановленням IMEI-номера терміналу, номера абонента у разі, якщо така особа починає сеанс голосового зв'язку. Відповідно, можливо здійснювати запис розмов цієї особи незалежно від того, яким терміналом або абонентським номером вона користується.

Відповідно до ч. 6 ст. 163 КПК України слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, якщо сторона кримінального провадження, крім обставин, передбачених ч. 5 цієї статті, доведе можливість використання як доказів відомостей, що містяться в цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів.

Доступ особи до речей і документів, які містять охоронювану законом таємницю, здійснюється в порядку, визначеному законом. Доступ до речей і документів, що містять відомості, які становлять державну таємницю, не може надаватися особі, що не має до неї допуску відповідно до вимог закону.

Слідчі судді місцевих судів повинні враховувати, що як у операторів зв'язку, так і у провайдерів мережі Інтернет можна отримати винятково інформацію, яка надійшла до них, а програмне забезпечення дозволяє зберігати її в пам'яті.

Зняття інформації (динамічної), яка буде надходити до них, належить до негласних слідчих дій. Зняття змісту непрочитаного і відправленого електронного листа з поштових скриньок серверів також належить до негласних слідчих дій і підпадає під категорію кореспонденції. Тому зняття такої інформації здійснюється в порядку глави 21 КПК України.

У пам'яті ОіПТ часто залишаються дані (SMS, MMS, e-mail та інші повідомлення) з текстовою, а також фото-, відеоінформацією, що передається як кореспонденція між особами. В свою чергу, норми Конвенції про захист прав людини і основоположних свобод щодо захисту поширюються на всі форми листування, насамперед на обмін листами та взагалі письмовими повідомленнями. Йдеться також про нові технології, такі як передавання повідомлень засобами приватного радіомовлення — так званими Citizen Band (англ. – «громадянський діапазон») або телефоном. За загальноприйнятим тлумаченням ст. 8 Конвенції закріплює принцип свободи кореспонденції (див. рішення Європейського суду з прав людини у справі «Andersson v. United Kingdom», 27 жовтня 1992 р.). Він стосується, зокрема, відправлення приватних, особистих листів, а також зберігання матеріалів або «предметів, що можуть належати до категорії кореспонденції» (пункт 7 рішення Європейського суду з прав людини у справі «Niemietz v. Germany», 23 листопада 1992 р.).

У принципі цей захист не поширюється на документи, які вже надійшли до одержувача і зберігаються ним. Відповідно, обшук і вилучення документів, що зберігаються в одержувача, мають вважатися такими, що не підпадають під дію пункту 1 ст. 8 Конвенції про захист прав людини і основоположних свобод. Такий підхід обґрунтовується в доктрині тим фактом, що ст. 8 Конвенції захищає можливість обмінюватися кореспонденцією, а не її матеріальний носій. Проте ця думка, очевидно, не має абсолютного характеру (див. рішення Європейського суду з прав людини у справі «Niemietz v. Germany», де Суд дійшов висновку, що ст. 8 Конвенції захищає професійні документи адвокатів).

Проте слід враховувати, що повідомлення, які надійшли на електронну пошту, SMS, MMS тощо, у тому числі і голосова пошта, повідомлення на автовідповідач, але не відкриті для прочитання (прослуховування, перегляду), підпадають під категорію кореспонденції у сенсі ст. 8 Конвенції про захист прав людини і основоположних свобод, доступ до них може бути здійснено лише на підставі ст. 261, ст. 263 КПК України.

Але якщо буде встановлено, що отримувач ознайомлений з їхнім змістом, вони можуть бути доступними для вилучення в порядку норм глави 15 КПК України.

Ініціаторами здійснення тимчасового доступу до інформації в мережі можуть бути учасники кримінального провадження – як з боку обвинувачення, так і з боку захисту, тобто визначені пунктом 19 ч. 1 ст. 3, ч. 1 ст. 160 КПК України. Слідчий має право звернутися із відповідним клопотанням за погодженням з прокурором (ч. 1 ст. 160 КПК України).

Клопотання повинно відповідати вимогам, передбаченим ч. 2 ст. 160 КПК України. У ньому зазначаються відомості про ОіПТ, якою інформацією вони володіють, яке значення вона має для встановлення обставин у кримінальному провадженні, можливість використання як доказів відомостей, що містяться в ній, та неможливість іншими способами довести обставини, які передбачається довести за їх допомогою.

Вимагається ретельно обґрунтувати необхідність вилучення цієї інформації, якщо відповідне питання порушується стороною кримінального провадження (ч. 2 ст. 160 КПК України).

При цьому слід ураховувати, що речами і документами, до яких забороняється доступ, є:

• листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги;

• об'єкти, які додані до такого листування або інших форм обміну інформацією (ст. 161 КПК України).

До клопотання додаються:

• витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, в рамках якого подається клопотання (ч. 6 ст. 132 КПК України);

• докази обставин, на які є посилання в клопотанні (ч. 5 ст. 132 КПК України).

Крім того, застосування заходів забезпечення кримінального провадження, в тому числі зняття інформації у ОіПТ, не допускається, якщо слідчий, прокурор не доведе, що:

• існує обґрунтована підозра щодо вчинення кримінального правопорушення такого ступеня тяжкості, що може бути підставою для застосування заходів забезпечення кримінального провадження;

• потреби досудового розслідування виправдовують такий ступінь втручання у права і свободи особи, про який ідеться у клопотанні слідчого, прокурора;

• може бути виконане завдання, з метою виконання якого слідчий, прокурор звертається із клопотанням (пункти 1–3 ч. 3 ст. 132 КПК України).

Для оцінки потреб досудового розслідування слідчий суддя або суд зобов'язаний врахувати можливість отримати речі і документи, які можуть бути використані під час судового розгляду для встановлення обставин у кримінальному провадженні, без застосування заходу забезпечення кримінального провадження (ч. 4 ст. 132 КПК України).

До клопотання слідчий або прокурор повинен також додати:

• відомості (копії довідки оператора, провайдера, протокол допиту, слідчих дій тощо) про ознаки, які дозволять ідентифікувати абонента шляхом уніфікації мереж (номери SIM-карти, IMEI, e-mail тощо);

• копії інших матеріалів, які мають важливе значення при розгляді клопотання – слідчий суддя, суд при постановленні ухвали в резолютивній частині повинен зазначати повні дані про особу, щодо якої отримується інформація (П.І.Б., місце роботи тощо);

• повний номер IMEI, назву оператора, провайдера, номери мобільних станцій, номер SIM-карти телефону з зазначенням коду України +38 (наприклад, +38 і номер SIM-карти телефону), точну електронну адреса мовою оригіналу із зазначенням розділових знаків, адреси IA, паролів SIM-карти, номера ICQ, оригінальної назви сайту, IP-адреси тощо.

Клопотання про застосування заходів забезпечення кримінального провадження на підставі ухвали слідчого судді подається до місцевого суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування (ч. 2 ст. 132 КПК України).

Після отримання клопотання слідчим суддею суд здійснює судовий виклик особи (фізичної, юридичної, у володінні якої знаходиться інформація (ч. 1 ст. 163 КПК України).

Клопотання розглядається слідчим суддею за участю сторони кримінального провадження, яка подала клопотання, та особи, у володінні якої знаходиться інформація (ч. 1 ст. 163 КПК України).

Згідно з ч. 4 ст. 163 КПК України слідчий суддя, суд розглядає клопотання за участю сторони кримінального провадження, яка подала клопотання, та представника оператора або провайдера. Неприбуття за судовим викликом представника сторони без поважних причин або неповідомлення нею про причини неприбуття не є перешкодою для розгляду клопотання.

Нормами глави 11 КПК України регламентується порядок викликів та приводів.

Згідно з ч. 8 ст. 135 КПК України особа має отримати повістку про виклик або бути повідомленою про нього іншим шляхом не пізніше ніж за 3 дні до дня, коли вона зобов'язана прибути за викликом. Повістка може бути надіслана також електронною поштою (ч. 2 ст. 136 КПК України) або іншими доступними методами (ч. 1 ст. 136 КПК України).

Згідно із пунктом 2 ч. 2 ст. 39 Закону «Про телекомунікації» ОіПТ зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом.

Крім того, як вже зазначалося, ОіПТ зобов'язані власним коштом встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і 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. ОіПТ зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу (ч. 4 ст. 39 Закону «Про телекомунікації»).

З урахуванням специфіки отриманої інформації, оперативності її використання при запобіганні, розкритті і розслідуванні кримінальних правопорушень слідчими суддями може бути в найкоротший час розглянуто клопотання учасників процесу, в тому числі слідчого і прокурора.

Було б доцільно судам здійснювати розгляд клопотань протягом робочого дня (за аналогією з ч. 1 ст. 248 КПК України – 6 годин), але не пізніше 3 діб з моменту їх реєстрації без участі представника оператора та провайдера (частини 2, 4 ст. 39 Закону «Про телекомунікації»).

Слідчий суддя, розглянувши клопотання, виносить ухвалу, в якій має бути зазначено:

1) прізвище, ім'я та по батькові особи, якій надається право тимчасового доступу до інформації;

2) дата постановлення ухвали;

3) положення закону, на підставі якого постановлена ухвала;

4) прізвище, ім'я та по батькові фізичної особи або найменування юридичної особи, які мають надати тимчасовий доступ до інформації;

5) назва, опис, інші відомості, які дають можливість визначити оператора та провайдера, номери засобів зв'язку, сайтів тощо, до яких повинен бути наданий тимчасовий доступ (ст. 164 КПК України).

Ухвала слідчого судді про розгляд клопотання про тимчасовий доступ до інформації, яка знаходиться у ОіПТ, оскарженню не підлягає.

Перелік ухвал слідчого судді, які підлягають оскарженню під час досудового розслідування, наведений у ст. 309 КПК України і є вичерпним.

Слід враховувати, що строк дії ухвали не може перевищувати одного місяця з дня її постановлення (пункт 7 ч. 1 ст. 164 КПК України).

Подання розглядається, а ухвала постановляється відповідно до вимог ст. 222 КПК України.

При внесенні клопотання з грифами «для службового користування», «таємно», «цілком таємно» слідчий, прокурор повинен пересвідчитися у наявності у судді допуску на роботу з цією категорією документів, а в суді – умов для роботи з такими документами відповідно до Закону України від 21 січня 1994 р. «Про державну таємницю» (в редакції Закону від 21 вересня 1999 р.).

Якщо інформація буде отримана щодо спеціальних суб'єктів (дипломатів, вищих державних службовців, народних депутатів, суддів тощо), слід враховувати вимоги спеціальних законів, які забезпечують їх імунітет, зокрема

про те, що всі оперативно-розшукові заходи, які здійснюються в межах законів «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про розвідувальні органи України», у тому числі для отримання інформації, яка знаходиться у ОіПТ, санкціонуються тільки слідчими суддями апеляційних судів.

Таким чином, порядок тимчасового доступу до інформації, яка знаходиться в ОіПТ, на підставі ухвали слідчих суддів місцевих судів України потребує законодавчого врегулювання (щодо видів інформації, строків та порядку розгляду клопотань).

ТАГІЄВ С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні.

У статті автор розглядає питання, пов'язані з тимчасовим доступом до інформації, яка зосереджена в операторів і провайдерів телекомунікацій, у ході кримінального провадження судами першої інстанції.

Ключові слова: оператор, провайдер, телекомунікації, інформація, тимчасовий доступ, кримінальне провадження.

ТАГИЕВ С. Временный доступ к информации, которая находится у операторов и провайдеров телекоммуникаций, в уголовном производстве.

В статье автор рассматривает вопросы, связанные с временным доступом к информации, которая сосредоточена у операторов и провайдеров телекоммуникаций, в ходе уголовного производства судами первой инстанции.

Ключевые слова: оператор, провайдер телекоммуникаций, информация, временный доступ, уголовное производство.

TAGIEV S. Temporary access to information which is at operators and providers of telecommunications in criminal proceedings.

The article examines issues related to temporary access to information that stored by telecommunication operators and providers in the course of criminal proceedings by the courts of first instance.

Key words: operator, a provider of telecommunications, information, temporary access, criminal proceedings.