УДК 343.1
DOI https://doi.org/10.32850/sulj.2022.1-2.22

ОСОБЛИВОСТІ ВИЛУЧЕННЯ ЗА ДОПОМОГОЮ ТЕХНІЧНИХ ЗАСОБІВ ІНФОРМАЦІЇ З МОБІЛЬНИХ ТЕРМІНАЛІВ ЗВ'ЯЗКУ (СМАРТФОНІВ) ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Лісніченко Д. В.

Стаття присвячена дослідженню питання про порядок вилучення інформації з мобільних терміналів зв'язку під час досудового розслідування. Зазначена тематика є актуальною у зв'язку зі стрімким розвитком науково-технічного прогресу, винайдення нових способів накопичення та передачі інформації. Впровадження нових підходів та методик отримання значущої для кримінального провадження інформації оптимізує та підвищить ефективність досудового розслідування.

Обґрунтована важливість інформації для кримінального провадження, яка знаходиться в мобільних терміналах зв'язку.

Проаналізовано кримінально-процесуальне законодавство та визначено, в рамках проведення яких процесуальних дій можливе отримання доступу до мобільних терміналів зв'язку з метою копіювання наявної в них інформації.

У статті запропоновано використовувати для копіювання інформації з мобільного терміналу зв'язку XRY (виробництва компанії MicroSystemation, Швеція) – програмно-апаратного комплексу, що призначений для проведення захищеного вилучення цифрових даних з різноманітних мобільних пристроїв. У зв'язку із застосуванням такого пристрою розглянуті два питання. Насамперед це порядок фіксації факту використання такого обладнання та аналіз норм кримінального процесуального законодавства, що регулюють ці вимоги.

Також у статті проаналізовано порядок використання вилученої інформації з мобільних терміналів зв'язку як доказів у кримінальному провадженні. Визначені проблемні питання використання такої інформації, а саме можливість використання як доказу інформації, що була скопійована з мобільного терміналу зв'язку, без вирішення питання про накладення арешту на такий мобільний термінал зв'язку.

Ключові слова: *кримінальне провадження, інформація, докази, мобільний термінал зв'язку, смартфон, XRY, тимчасове вилучення майна, арешт майна.*

Lisnichenko D. V. Features of extraction by technical means of information from mobile communication terminals (smartphones) during criminal proceedings

The article is devoted to the study of the procedure for removing information from mobile communication terminals during the pre-trial investigation. This topic is relevant in connection with the rapid development of scientific and technological progress the invention of new ways of collecting and transmitting information. Introduction of new approaches and methods of obtaining information relevant to criminal proceedings will optimize and increase the efficiency of pre-trial investigation.

The importance of information for criminal proceedings, which is located in mobile communication terminals, is substantiated.

The criminal procedure legislation has been analyzed and it has been determined within the framework of which procedural actions it is possible to gain access to mobile communication terminals in order to copy the information available in them.

The article proposes to use for copying information from the mobile communication terminal XRY (manufactured by MicroSystemation, Sweden), software and hardware designed to securely extract digital data from a variety of mobile devices. There are two issues with this device. The first is the procedure for recording the use of this equipment and analysis of the rules of criminal procedure governing these requirements.

The article also analyzes the procedure for using the extracted information from mobile communication terminals as evidence in criminal proceedings. Identify the problematic issues of using such information, namely the possibility of using as evidence information that was copied from a mobile communication terminal, without resolving the issue of seizure of this mobile communication terminal.

Key words: *criminal proceedings, information, evidence, mobile communication terminal, smartphone, XRY, temporary seizure of property, seizure of property.*

Постановка проблеми та її актуальність. Нестримний розвиток науково-технічного прогресу впливає на всі без виключення сфери людської життєдіяльності. Особливо це стосу-

ється комунікації та зв'язку. Ми маємо на увазі мобільні термінали зв'язку (смартфони), які перетворились з простих засобів комунікації на пристрої надширокого спектра застосування, що дозволяють здійснювати: доступ до інформації; платіжні операції; навчання; трудову діяльність; спілкування; передачу інформації; фото- та відеофіксування та багато іншого. Оскільки зазначений термінал (смартфон) здійснює таку кількість операцій, останній накопичує величезний масив інформації про свого власника. Зазначений пристрій може «розповісти» про коло знайомств та спілкування, фінансові операції, місця перебування, інтереси та інше про свого власника.

У рамках кримінального провадження доступ до зазначеної інформації правоохоронні органи можуть отримати лише під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій. Водночас варто зазначити, що повнота та якість отримання відповідної інформації залежить від застосування науково-технічних засобів та навичок їх застосування.

Аналіз останніх досліджень і публікацій. Використання науково-технічних засобів у діяльності з розкриття та розслідування злочинів висвітлені у наукових дослідженнях В.П. Бахіна, Р.С. Бєлкіна, Г.І. Грамовича, І.А. Ієрусалимова, А.В. Іщенка, Н.С. Карпова, М.І. Клименка, В.В. Коваленка, В.С. Кузьмічова, М.В. Салтевського, В.Ю. Шепітька.

Загальні принципи використання науково-технічних засобів та даних, одержаних шляхом їх використання в кримінальному провадженні, досліджено у працях: О.М. Бандурки, О.В. Бауліна, Б.Т. Безлєпкіна, П.Д. Біленчука, В.Г. Гончаренка, Ф.К. Діденка, А.Я. Дубінського, А.В. Іщенка, О.А. Леві, Н.С. Карпова, В.С. Кузьмічова, О.М. Ларіна, З.М. Ломако, П.А. Лупинської, А.О. Ляша, Г.М. Міньковського, М.Г. Несена, В.Т. Нора, Ю.М. Оропая, Е.А. Разумова, М.А. Селіванова, В.М. Тертишника, С.А. Шейфера, В.П. Шибіки, Р.Х. Якупова та ін.

Водночас через надзвичайно динамічний розвиток інформаційних технологій, розвиток функціональних можливостей гаджетів є необхідність у постійному вдосконаленні методик з виявлення та використання інформації, яка міститься в мобільних терміналах зв'язку.

Звичайно, це дуже цінна інформація для правоохоронних органів в аспекті їхньої діяльності, але безконтрольне та неврегульоване використання зазначеної інформації невідворотно призведе до порушень конституційних прав особи та громадянина.

Законодавчі органи різних країн, усвідомлюючи зазначені ризики, намагаються врегулювати та напрацювати порядок доступу правоохоронних органів до інформації, яка міститься в мобільному терміналі зв'язку (смартфоні).

Не виключенням є і наша країна. Згідно із Законом України № 2213-VIII від 16.11.2017 р., частину другу статті 168 КПК України було доповнено абзацами третім та четвертим, а саме:

«Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

У разі необхідності слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста» [1].

Варто відзначити прогресивність зазначеної норми, що на законодавчому рівні дозволяє здійснювати копіювання інформації, що знаходиться в мобільному терміналі зв'язку.

Основний спосіб здобути необхідну інформацію – отримати доступ до мобільного пристрою та аналіз даних, які містяться в мобільному пристрої.

Насамперед варто зазначити, що чинне законодавство передбачає доволі широкий перелік процесуальних інструментів, які дають доступ до інформації, що міститься в мобільному терміналі зв'язку. Зазначений доступ можна отримати як у рамках проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій, так і в рамках застосування заходів забезпечення кримінального провадження.

Аналіз Глави 20, яка містить у собі перелік та порядок застосування слідчих (розшукових) дій, дозволяє стверджувати, що слідчими (розшуковими) діями, процесуальний порядок проведення яких передбачає вилучення речей (тобто отримання доступу), є обшук та огляд [1].

З позиції ефективного розслідування зауважимо, що як у минулому, так і нині обшук є однією з найбільш ризикованих і водночас однією з найбільш плідних слідчих (розшукових) дій, що включає і вилучення майна. Адже майже жодне розслідування не може обійтися без обшуку з тієї простої причини, що саме обшук передбачає дії слідчого щодо пошуку або збору речових доказів [2].

Водночас обшук та огляд мають суттєві відмінності. Так, огляд місця події може проводитись до моменту, з якого розпочинається кримінальне провадження (ч. 2 ст. 214 КПК України), тобто до моменту внесення відомостей до ЄРДР, а провадження обшуку допускається лише за наявності кримінального провадження.

Одна з основних відмінностей обшуку від огляду полягає в меті їх застосування. Так, в обшуку вона більш конкретна, але значно вужча за мету огляду, в ході якого акцентується увага на всебічне дослідження, детальну фіксацію як обстановки, довколишнього середовища, так і об'єкта, що оглядається, можливо, з подальшим його вилученням.

Аналогічну можливість доступу дає і застосування деяких негласних слідчих (розшукових) дій. Аналіз норм глави 21 КПК України, яка закріплює коло негласних слідчих (розшукових) дій, дозволяє стверджувати, що можливість доступу до мобільних терміналів зв'язку є у ході проведення таких негласних слідчих (розшукових) дій:

1) виїмки кореспонденції, на яку накладено арешт (ст.ст. 261 і 262 КПК України);

2) контролю за вчиненням злочину (ст. 271 КПК України);

3) виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України).

Також такий доступ можливо здійснити під час затримання (особистого обшуку), тимчасового доступу до речей та документів.

У разі вилучення мобільного терміналу зв'язку за процедурою тимчасового вилучення майна передбачається надалі звернення до слідчого судді з клопотанням про накладення арешту на зазначений мобільний пристрій.

Однак розвиток науково-технічного прогресу натепер дозволяє отримати доступ до необхідної інформації в мобільному пристрої, не здійснюючи тимчасового вилучення майна з подальшим накладенням арешту на майно, а маючи у своєму розпорядженні мобільний пристрій, лише на декілька хвилин у рамках проведення затримання, огляду чи обшуку.

Одним з пристроїв, які можуть здійснювати копіювання інформації, яка знаходиться на мобільному пристрої, є XRY (виробництва компанії MicroSystemation, Швеція). Програмно-апаратний комплекс призначений для проведення захищеного вилучення цифрових даних з різноманітних мобільних пристроїв, таких як смартфони, GPS-навігатори, 3G-модеми, портативні аудіоплеєри, планшетні комп'ютери. В результаті дослідження телефонів створюються захищені від несанкціонованого доступу звіти, які можна вивести на друк або записати на компакт-диск [3].

Звичайно, в рамках розслідування кримінальних правопорушень у разі тимчасового вилучення мобільних пристроїв особу, яка здійснила таке вилучення, насамперед цікавить саме інформація, яка знаходиться на мобільному пристрої, а не сам пристрій. Отже, відпадає необхідність у майбутньому звертатись до слідчого судді з клопотанням про накладення арешту на мобільний пристрій з метою отримання можливості аналізу та використання як доказу інформації, що знаходилась на мобільному пристрої.

Водночас у разі здійснення таких дій виникають два дискусійних питання: порядок фіксації таких дій та порядок використання вилученої інформації.

Хочемо спочатку обговорити питання фіксації застосування технічних засобів.

Низка науковців схиляються до думки, що факт застосування технічного засобу для копіювання інформації з мобільного терміналу зв'язку потребує винесення окремої постанови. Так, Б.Д. Леонов зазначає, що, крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу про проведення НС(Р)Д, у разі використання комп'ютерних технологій у ньому необхідно фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення. При цьому слід враховувати, що відповідно до ч. 1 ст. 107 КПК України **рішення про фіксацію процесуальної дії за допомогою технічних засобів під час досудового розслідування приймає особа, яка проводить відповідну процесуальну дію.** Таким чином, оскільки положеннями КПК України прямо передбачено, що рішення про фіксацію процесуальної дії за допомогою технічних засобів приймається особою, яка проводить відповідну процесуальну дію, то відповідно до ч. 3 ст. 110 КПК України особа, яка проводить НС(Р)Д, повинна винести відповідну постанову про фіксацію процесуальної дії за допомогою технічних засо-

бів. При цьому слідчий (оперативний працівник) повинен вказати у цій постанові ідентифікаційні ознаки технічних засобів, які будуть використані під час проведення НС(Р)Д. Посилання прокурора на ту обставину, що ухвалою слідчого судді, який надав дозвіл на проведення НС(Р)Д, уже надано дозвіл на її проведення і винесення постанови відповідно до ч. 1 ст. 107 КПК України недоцільне, не може прийматися до уваги, оскільки ухвала слідчого судді лише **надає дозвіл слідчому та/або прокурору на проведення конкретної** НС(Р)Д. Проте реалізація цього рішення залежить від волі слідчого чи прокурора. Отримавши такий дозвіл від слідчого судді, прокурор залежно від обставин кримінального провадження, може не проводити відповідну НС(Р)Д. Крім того, в ухвалі слідчого судді не відображаються технічні засоби, які будуть використані для проведення НС(Р)Д, оскільки такої інформації у слідчого судді немає і не може бути на момент прийняття ним такого рішення. Невинесення відповідної постанови про фіксацію процесуальної дії за допомогою технічних засобів є істотним порушенням ч. 1 ст. 107 КПК України, що тягне за собою недопустимість такого доказу, оскільки такий доказ **отриманий не в порядку, передбаченому КПК України.** Таким чином, для використання технічних засобів, у тому числі й комп'ютерних технологій під час проведення НС(Р)Д, вважаємо за необхідне обов'язкове винесення відповідної постанови про фіксацію НС(Р)Д за допомогою відповідних технічних засобів з урахуванням положень ч. 1 ст. 252 та ч. 1 ст. 104 КПК України [4].

Ми не можемо погодитись з такою позицією. Насамперед варто зазначити, що автор апелює до вимог статті 107 КПК України, однак остання регулює питання щодо застосування під час процесуальної дії технічних приладів саме для фіксації останньої, а не питання застосування технічних засобів для безпосереднього проведення процесуальної дії, в тому числі і НС(Р)Д. Звичайно, факт застосування технічних засобів передбачає необхідність фіксації його застосування в протоколі процесуальної дії. Однак водночас вважаємо безпідставною ідею щодо необхідності винесення окремої постанови про застосування. Це все одно що виносити окрему постанову на кожний засіб, що використовує криміналіст під час огляду місця події. Також зазначена практика, з нашої точки зору, створює зайву бюрократизацію кримінального провадження та жодним чином не забезпечує своїм існуванням більш суворого дотримання прав та законних інтересів учасників кримінального провадження.

Водночас ми абсолютно погоджуємось з твердженням про детальне зазначення характеристик технічного засобу, що використовувався під час копіювання інформації з мобільного терміналу зв'язку. Так, у разі використання комп'ютерних технологій під час проведення процесуальної дії в протоколі необхідно зазначати: 1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника; 2) серійний номер комп'ютерної програми, пристрою, обчислювальної техніки або програмного забезпечення; 3) наявний стан зношеності або будь-яких дефектів зовнішнього вигляду чи у роботі використаного технічного засобу, пристрою, обчислювальної техніки, програмного забезпечення (визначається зовнішнім візуальним оглядом слідчого чи оперативного працівника); 4) умови, у яких було використано технічний засіб, пристрій, обчислювальну техніку або програмне забезпечення, а також дату й точний час; 5) всю інформацію в цифровому вигляді, яка являє процесуальний або оперативний інтерес незалежно від того, на якому носії вона знаходиться, бажано оглянути в присутності спеціаліста й понятих, після чого скопіювати її на матеріальний носій, який повинен бути долучений до протоколу проведення процесуальної дії незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації [5, с. 303]; 6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диску комп'ютера, необхідно користуватись програмним забезпеченням для побітового копіювання інформації (наприклад, програми «SMART», «NED», «FTK», «dd» тощо), а після копіювання до протоколу проведення НС(Р)Д необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено. Використання вказаних та інших вимог положень чинного КПК України слугуватиме більш ефективному застосуванню новітніх технологій у досудовому розслідуванні, зокрема під час проведення негласних слідчих (розшукових) дій, а також під час їх оформлення як слідчими, так і працівниками оперативних підрозділів, що виконують такі дії за їх дорученням. Однак окреслені питання потребують окремого дослідження або наукового вивчення [6, с. 87].

Що стосується подальшого порядку використання отриманої під час досудового розсліду-

вання інформації, то тут теж є певні невизначені аспекти, на які ми хотіли б звернути увагу.

Виникають такі питання: чи буде доказ на підставі отриманої шляхом копіювання інформації з мобільного пристрою допустимим, якщо слідчий не отримав дозволу суду на арешт джерела цієї інформації як підтвердження законності її отримання? Якщо в кримінальному провадженні як доказ буде використовуватись інформація з мобільного пристрою, то чи вказаний мобільний пристрій повинен знаходитись у фактичному законному володінні сторони обвинувачення?

Крім того, деякі науковці зазначають, що відповідно до ч. 1 ст. 258 КПК України ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді. Відповідно до ч. 1 ст. 264 КПК України пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді. Таким чином, без ухвали слідчого судді ніхто не має права провести огляд комп'ютерної техніки чи мобільного телефону особи з відома чи без відома власника такої інформаційної системи. На практиці ж системою є така ситуація, коли слідчий, вилучивши під час обшуку мобільний телефон чи комп'ютер особи, не звертаючись до слідчого судді за дозволом на зняття інформації з електронних інформаційних систем, проводить огляд таких пристроїв, складає протокол огляду і використовує отриману таким чином інформацію як доказ у кримінальному провадженні. Таким чином, слідчий прямо порушує ч. 1 ст. 258 та ч. 1 ст. 264 КПК України. Відповідно, в разі відсутності дозволу слідчого судді на зняття інформації з електронних інформаційних систем особи, але отримання з даних інформаційних систем інформації шляхом огляду мобільного телефону чи комп'ютера, яку слідчий відобразив у протоколі огляду, то отримана таким чином інформація не може бути визнана допустимим доказом у кримінальному провадженні, оскільки такий доказ отриманий не в порядку, передбаченому Кримінальним процесуальним кодексом України [7].

Ми не зовсім згодні з такою позицією. Згідно з ч. 1 статті 246 КПК України, негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню. Тобто особа не знає про факт проведення таких дій. Водночас коли мобільний пристрій вилучається під час затримання чи обшуку, факт вилучення мобільного пристрою є явним, тому, на нашу думку, огляд такого мобільного пристрою не може вважатись негласною слідчою розшуковою дією, яка передбачає отримання дозволу слідчого судді.

Свою позицію, з якою ми погоджуємось, щодо порядку отримання інформації, яка міститься на мобільному терміналі зв'язку, та оцінки її допустимості в кримінальному провадженні, зазначив Верховний Суд України у своїй постанові № 727/6578/17 від 9 квітня 2020 року, де колегією суддів Другої судової палати Касаційного кримінального суду визнав безпідставним твердження захисника про те, що під час досудового розслідування було здійснено незаконний (без постанови слідчого судді) доступ до відомостей з електронних інформаційних мереж, який оформлений як протокол огляду предмета – телефону.

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, розміщенням 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.

Що ж стосується інформації, яка була наявна в мобільному телефоні, 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 такому 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 під час розгляду такого кримінального провадження [8].

Все вищезазначене свідчить про необхідність подальшого законодавчого регулювання порядку отримання інформації, яка міститься в мобільних терміналах зв'язку, її аналізу та використання в кримінальному провадженні.

Література

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-17: станом на 20.10.2021 р. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 21.10.2021).

2. Благодир А.А. Застосування примусу під час провадження слідчих дій : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, НУВС. 2009. 20 с.

3. Виявлення, фіксація та вилучення криміналістично значущої інформації з мобільних пристроїв під час розслідування кримінальних правопорушень / А.В. Холостенко, Д.С. Афонін, К.Ю. Ісмайлов, Д.В. Лісніченко, О.І. Постол. Одеса : Одеський державний університет внутрішніх справ, 2018. 38 с.

4. Леонов Б.Д., Серьогін В.С. Кримінально-правова протидія незаконній діяльності зі спеціальними технічними засобами негласного отримання інформації. *Інформація і право*. 2016. № 2(17). С. 139–144.

5. Доля Е.А. Формирование доказательств на основе результатов оперативно-розыскной деятельности : монография. Москва : Проспект, 2009. 357 с.

6. Юхно О.О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2 (73). С. 86–95.

7. Андрій Леонов, суддя Бабушкінського районного суду м. Дніпропетровська «Особливості проведення негласних слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень». URL: https://zib.com.ua/ua/136530-osoblivosti_provedennya_nsrd_v_kriminalnomu_provadzhenni.html.

8. Постанова ВСУ № 727/6578/17 від 09.04.2020. URL: http://reyestr.court.gov.ua/Review/88749345.

Лісніченко Д. В.,
кандидат юридичних наук,
викладач кафедри кримінального процесу
Одеського державного університету
внутрішніх справ