

УДК 343.23:343.98:004.738.5

DOI <https://doi.org/10.32782/ln.2024.24.46>**Філімонов М.В.,***аспірант кафедри кримінального процесу**Національний університет**«Одеська юридична академія»*

ОКРЕМІ ПИТАННЯ ПРИЗНАЧЕННЯ ЕКСПЕРТИЗИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРОУШЕНЬ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Актуальність проблематики призначення та проведення судових експертиз при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі, зумовлена стрімкою цифровізацією суспільних відносин та зростанням ролі інформаційно-комунікаційних технологій у повсякденному житті. Натепер значна частина кримінальних правопорушень, пов'язана з використанням комп'ютерних систем, телекомунікаційних мереж, мобільних пристроїв, мережі Інтернет та інших високих інформаційних технологій, що об'єктивно ускладнює процес збирання та перевірки доказів під час кримінального провадження. За таких умов, «традиційні» процесуальні засоби доказування нерідко виявляються недостатніми без застосування спеціальних знань у сфері інформаційних технологій.

Судові експертизи у цьому контексті набувають ключового значення, оскільки саме вони забезпечують можливість належної ідентифікації цифрових слідів кримінального правопорушення, встановлення механізму протиправних дій, джерел походження електронної інформації, а також зв'язку між конкретною особою та вчиненим діянням. Комп'ютерно-технічні, трасологічні, експертизи електронних комунікацій та інші види експертиз дозволяють забезпечити належність та допустимість технічно складних цифрових даних як доказів.

Враховуючи специфіку цифрових доказів, які характеризуються нематеріальністю,

високою вразливістю до змін, можливістю швидкого знищення або модифікації, а також залежністю від спеціального програмного та апаратного забезпечення, саме судові експертизи здатні забезпечити достовірність та відтворюваність цифрової інформації.

Таке значення спеціальних знань при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі робить відповідну проблематику комплексною та різноаспектною. Саме тому, у межах нашого дослідження ми ставимо за мету більш детально розглянути проблеми призначення експертизи електронних комунікацій як одного із найпоширеніших видів судових експертиз при розслідуванні розглядуваної категорії кримінальних правопорушень, з'ясувати її можливості та перспективи вирішення окремих найбільш дискусійних питань, пов'язаних із її проведенням.

До питання призначення судових експертиз, у тому числі, тих, які проводяться у кримінальних провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі у сучасній кримінальній процесуальній доктрині звертались І. Басиста, Л. Белік, Л. Будник, А. Воробчак, В. Гусева, О. Дуфенюк, О. Дульський, І. Каланча, В. Кисельов, А. Коваленко, В. Коршенко, В. Колесник, Г. Крет, А. Кунтій, Є. Лук'янчиков, І. Пиріг, Ю. Пілюков, В. Попелюшко, О. Саїнчин, О. Самойленко, Е. Сімакова-Єфремян, Р. Степанюк, С. Стратонов, Б. Теплицький, О. Тищенко, Ю. Циганюк, Ю. Чорноус,

К. Шуневич, М. Щербаковський. У контексті проведення експертизи електронних комунікацій окремої уваги заслуговує дисертаційне дослідження В.А. Коршенка «Теоретичні та методичні основи судової телекомунікаційної експертизи» (м. Харків, 2017). Втім, динаміка розвитку інформаційних технологій та тенденції правозастосування вказують на необхідність подальшого наукового осмислення питань призначення цього виду експертиз, зокрема, у контексті саме тих кримінальних правопорушень, що вчиняються у кіберпросторі.

Нормативні основи експертизи електронних комунікацій, як і всіх судових експертиз закладені в Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої Наказом Міністерства юстиції України від 08.10.1998 № 53/5 (далі – Наказ) [1]. У п. 14.2 Наказу основними завданнями відповідного роду експертних досліджень визначені: 1) визначення характеристик та параметрів мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів та випромінювальних пристроїв; 2) встановлення фактів та способів передачі (отримання) інформації з використанням мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 3) встановлення фактів та способів доступу до мереж, ресурсів та інформації у сфері електронних комунікацій; 4) визначення технічних чинників якості надання електронних комунікаційних послуг на рівні їх споживання; 5) встановлення конфігурації та робочого стану мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 6) встановлення типу, марки, моделі та інших класифікаційних категорій мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв; 7) дослідження алгоритмів обробки інформації та її захисту в мережах електронних комунікацій та їх

складових, радіообладнанні, радіоелектронних засобах, випромінювальних пристроях.

Говорячи про значення цієї експертизи для кримінального провадження, В.А. Коршенко зазначає, що воно полягає у дослідженні засобів і систем телекомунікації та відповідної інформації з метою встановлення слідів злочину та криміналістично значущої інформації в об'єктах, виявлених під час проведення слідчих (розшукових) дій; визначення інформації, зібраної під час проведення негласних слідчих (розшукових) дій і знятої з транспортних телекомунікаційних мереж та отриманої у ході процесуальних дій дистанційного кримінального провадження з використанням технологій телекомунікації [2, с. 10].

Водночас, доволі часто у правозастосовній практиці перед експертами ставиться також й питання щодо того, чи взагалі відносяться певні пристрої до електронно-обчислювальної техніки і які функції вони здатні виконувати. Наприклад, в ухвалі слідчого судді Індустріального районного суду м. Дніпропетровська при призначенні судової телекомунікаційної експертизи перед експертом були поставлені такі питання: 1) Чи відносяться надані на дослідження пристрої до електронно-обчислювальної машини (ЕОМ, комп'ютер)? Якщо так, то за якими ознаками?; 2) Чи може надані на дослідження пристрої виконувати функції кодграббера-ретранслятора або в просторіччі «удочка», чи «довга рука»? Якщо так, чи може наданий на дослідження пристрій виконувати дії по ретрансляції сигналу автомобільної системи типу «Keyless Go» або «SmartKey» (система комфортного доступу)?; 3) Чи може надані на дослідження пристрої виконувати функції пригнічення електронних сигналів, якщо так до якого типу відноситься? [3]

Однак окрім технічних характеристик певного засобу, перед експертами в межах експертизи електронних комунікацій доволі часто ставляться також й питання щодо встановлення IMEI зазначеного пристрою; номери мобільного оператора в наявній SIM-карті;

встановлення номера мобільного оператора в наявній в технічному пристрої SIM карті [4].

Як показує аналіз судової практики, відповідний вид експертних досліджень є доволі поширеним у кримінальних провадженнях за ст. 176 Кримінального кодексу України (Порушення авторського права і суміжних прав). У відповідній категорії кримінальних проваджень аналізований вид експертизи призначається, як правило, з метою з'ясування того чи можуть певні апаратні засоби об'єднуватись у телекомунікаційну мережу, встановлення шляхів маршрутизації даних тощо. Для прикладу того, які питання можуть бути поставлені при призначенні експертизи електронних комунікацій під час досудового розслідування кримінального правопорушення, передбаченого с. 176 КК України наведемо перелік питань, які були поставлені експертом в ухвалі слідчого судді Галицького районного суду м. Львова від 17 січня 2019 року: 1) Чи могли вищезазначені апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками?; 2) Які шляхи маршрутизації даних у вищевказаній телекомунікаційній системі?; 3) Чи можливо використання вищевказаних телекомунікаційних засобів для прийому та передачі супутникових сигналів?; 4) Чи можливо використання зазначеного телекомунікаційного обладнання для трансляції наступних телеканалів «1+1», «2+2», «TeT», «Плюс Плюс», «Бігуді», «Уніан», «СТБ», «ICTV», «Новий канал», «М-1», «М-2», «ОЦЕ ТБ», «ТРК Україна», «Футбол 1» та «Футбол – 2»? [5]

Окремо слід наголосити й на тому, що нерідко при розслідуванні кримінальних правопорушень, вчинених у кіберпросторі призначаються, у тому числі, й комплексні комп'ютерно-технічні експертизи та експертизи електронних комунікацій. Така експертиза призначається з метою всебічного дослідження цифрової інформації та процесів електронного обміну даними, коли встановлення обставин кримінального провадження

потребує спеціальних знань одночасно у сфері інформаційних технологій і телекомунікацій. Її комплексний характер зумовлений тим, що відомості про кримінальне правопорушення, вчинене у кіберпросторі зазвичай містяться як на матеріальних носіях інформації (комп'ютери, мобільні пристрої, сервери), так і можуть мати нематеріальний характер у вигляді інформації про передавання даних у мережах електронного зв'язку. Наприклад, можливості такої експертизи можуть включати в себе одночасне дослідження програмного забезпечення, мережових налаштувань, лог-файлів, історії доступу та використання інформаційних систем та встановлення зв'язку між конкретними пристроями, абонентами, обліковими записами та подіями у цифровому середовищі. Завдяки такій експертизі з'являється можливість інтегрувати технічні та телекомунікаційні аспекти цифрових слідів у єдину, процесуально значущу систему доказів.

Як приклад, ухвалою слідчого судді Кіровського районного суду м. Кропивницького про призначення комплексної (комп'ютерно-технічної та у сфері телекомунікаційних систем і мереж) експертизи у кримінальному провадженні перед експертом були поставлені, зокрема, такі питання: 1) чи інстальовано на «Smart TV BOX X96 mini» (MAC:900EB30ADDF3) Android додаток «fry!TV»?; 2) який принцип дії та функціональні можливості Android додаток «fry!TV»?; 3) чи є можливість, використовуючи Android додаток «fry!TV» перегляд (ретрансляція, трансляція) телеканалів «1+1», «2+2», «TET», «Плюс Плюс», «Бігуді», «УНІАН», «Paramount Comedy» та «KVARTAL TV», якщо так, то яким саме чином?; 4) яка мережева активність даного додатку, адреса та спосіб передачі інформації?; 5) чи є на веб-ресурсі «<https://4pda.ru>» Android додаток «fry!TV» та чи є він ідентичний додатку, що інстальовано на «Smart TV BOX X96 mini» (MAC:900EB30ADDF3)? [6]

В інших ухвалах, якими було призначено комплексну комп'ютерно-технічну та у сфері

телекомунікаційних систем і мереж експертизу перед експертами також ставилось питання про діапазон IP-адрес, до яких входить IP-адреса, на якій розміщується веб-сайт/ресурс [7], а також наявність ознак несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки блокування інформації [8].

Процесуальний порядок призначення експертизи електронних комунікацій загалом не має специфічних особливостей: сторона обвинувачення залучає експерта для проведення такої експертизи за дорученням, а сторона захисту на договірних засадах або шляхом звернення до слідчого судді у порядку ст. 244 КПК України (ч. 1 ст. 244 КПК України).

Як показує аналіз судової практики, при зверненні до слідчого судді та подальшому розгляді клопотання, сторона захисту загалом стикається із доволі традиційними для даної категорії клопотань проблемами. Це зокрема, стосується доказування неможливості самостійного залучення експерта та наявності об'єктивних сумнівів щодо правильності висновків та їх обґрунтованості [9], а також визначення об'єктів для експертного дослідження [10]. Крім того, виникають й питання щодо правильності тлумачення підстав залучення експерта, визначених ч.1 ст. 244 КПК України, у тому числі в ситуаціях, коли об'єкт для експертного дослідження не перебуває у володінні сторони захисту. До прикладу, в одній із ухвал слідчим суддею було зазначено наступне: «Так, захисник посиляється на неможливість надати експерту на дослідження телекомунікаційний засіб, оскільки він вилучений в ході проведення обшуку та перебуває у слідчого».

Однак, залучення експерта та надання йому об'єкта експертизи не є тотожними поняттями. Відмови слідчого у наданні експерту для дослідження вилученого телекомунікаційного засобу матеріали клопотання не містять» [11].

У цьому контексті слід зауважити, що норми ст. 244 КПК України не вимагають від сторони захисту попередньо звертатись до слідчого або прокурора з клопотанням про проведення експертизи. Крім того, у ч.8 ст. 244 КПК України передбачено, що «при задоволенні клопотання про залучення експерта слідчий суддя у разі необхідності має право за клопотанням особи, яка звернулася з клопотанням про залучення експерта, вирішити питання про отримання зразків для експертизи відповідно до ст. 245 КПК України». Однак, тягар доказування обставин, передбачених ч.1 ст. 244 КПК України, безумовно покладатиметься на сторону захисту. Її завданням при цьому безперечно буде й формулювання питань, які необхідно поставити експерту та доведення доцільності проведення відповідного експертного дослідження.

Проведене дослідження дає підстави стверджувати, що експертиза електронних комунікацій є одним із ключових засобів доказування у кримінальних провадженнях щодо кримінальних правопорушень, вчинених у кіберпросторі. Її значення зумовлене як об'єктивною складністю ідентифікації та вилучення цифрових слідів кримінального правопорушення, так і необхідністю використання спеціальних знань для встановлення технічних характеристик електронних засобів, способів передавання інформації, функціональних можливостей телекомунікаційних систем та взаємозв'язку між окремими подіями у цифровому середовищі.

Аналіз правозастосовної практики засвідчує, що завдання експертизи електронних комунікацій мають широкий і багатоаспектний характер: від ідентифікації технічних параметрів пристроїв і мереж до встановлення фактів доступу, маршрутизації даних, передачі інформації та функціонального призначення телекомунікаційного обладнання. Особливе практичне значення цей вид експертизи має у кримінальних провадженнях, де об'єктом дослідження є складні технічні системи або програмно-апаратні комплекси.

Це стосується, зокрема, кримінальних правопорушень, пов'язаних із порушенням авторського права і суміжних прав, несанкціо-

ваним доступом до інформаційних систем чи незаконним використанням телекомунікаційних мереж.

Анотація

Стаття присвячена аналізу актуальних проблем призначення та проведення експертизи електронних комунікацій під час досудового розслідування кримінальних правопорушень, вчинених у кіберпросторі. Обґрунтовується, що стрімка цифровізація суспільних відносин і широке використання інформаційно-комунікаційних технологій зумовлюють трансформацію механізмів злочинної діяльності та ускладнюють процес доказування. У цьому контексті наголошується на зростанні ролі спеціальних знань, без застосування яких традиційні процесуальні засоби не здатні забезпечити належне збирання, перевірку та оцінку електронних доказів.

Автор досліджує нормативні та науково-теоретичні засади експертизи електронних комунікацій, зокрема положення Інструкції про призначення та проведення судових експертиз та експертних досліджень, а також підходи, сформовані у кримінальній процесуальній доктрині. Значну увагу приділено аналізу завдань цього виду експертизи, її можливостей щодо встановлення технічних характеристик телекомунікаційних мереж і пристроїв, фактів та способів передавання інформації, доступу до електронних ресурсів, а також функціонального призначення програмно-апаратних засобів. Окремо розглядається практика призначення комплексних комп'ютерно-технічних і телекомунікаційних експертиз та коло питань, що ставляться перед експертами у відповідних кримінальних провадженнях.

Досліджено особливості процесуального порядку залучення експерта стороною обвинувачення та стороною захисту, а також типові проблеми, з якими стикається сторона захисту при зверненні до слідчого судді у порядку ст. 244 КПК України. Проаналізовано судову практику щодо тлумачення окремих підстав призначення експертизи, вилучення об'єктів експертного дослідження та розподілу тягаря доказування.

Автор доходить висновку, що завдання експертизи електронних комунікацій мають широкий і багатоаспектний характер: від ідентифікації технічних параметрів пристроїв і мереж до встановлення фактів доступу, маршрутизації даних, передачі інформації та функціонального призначення телекомунікаційного обладнання. Особливе значення цей вид експертизи має у кримінальних провадженнях, де об'єктом дослідження є складні технічні системи або програмно-апаратні комплекси.

Ключові слова: кіберпростір, електронні докази, судова експертиза, експертиза електронних комунікацій, комп'ютерно-технічна експертиза, досудове розслідування, спеціальні знання, слідчі (розшукові) дії.

Filimonov M.V. Certain Issues of Appointing Forensic Examination of Electronic Communications during the Pre-Trial Investigation of Criminal Offences Committed in Cyberspace

Summary

The article is devoted to the analysis of current problems related to the appointment and conduct of forensic examinations of electronic communications during the pre-trial investigation of criminal offences committed in cyberspace. It is substantiated that the rapid digitalisation of social relations and the widespread use of information and communication technologies lead to the transformation of criminal activity mechanisms and significantly complicate the process of proof. In this context, emphasis is placed on the growing role of specialised knowledge, without which traditional pro-

cedural means are unable to ensure the proper collection, verification and evaluation of electronic evidence.

The author examines the regulatory and scientific-theoretical foundations of forensic examination of electronic communications, in particular the provisions of the Instruction on the Appointment and Conduct of Forensic Examinations and Expert Studies, as well as the approaches developed within criminal procedural doctrine. Considerable attention is paid to the analysis of the tasks of this type of examination and its capabilities in establishing the technical characteristics of telecommunication networks and devices, the facts and methods of information transmission, access to electronic resources, as well as the functional purpose of software and hardware systems. Special focus is given to the practice of appointing комплексні computer-technical and telecommunication forensic examinations and to the range of questions posed to experts in relevant criminal proceedings.

The procedural specifics of engaging an expert by the prosecution and the defence are analysed, along with typical problems faced by the defence when applying to the investigating judge pursuant to Article 244 of the Criminal Procedure Code of Ukraine. Judicial practice concerning the interpretation of certain grounds for the appointment of forensic examinations, the determination of objects of expert research, and the allocation of the burden of proof is also examined.

The author concludes that the tasks of forensic examination of electronic communications are broad and multidimensional, ranging from the identification of technical parameters of devices and networks to the establishment of facts of access, data routing, information transmission and the functional purpose of telecommunication equipment. This type of forensic examination is of particular importance in criminal proceedings where the objects of research are complex technical systems or software and hardware complexes.

Key words: cyberspace, electronic evidence, forensic examination, forensic examination of electronic communications, computer-technical forensic examination, pre-trial investigation, specialised knowledge, investigative (search) actions.

Список використаних джерел:

1. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: Наказ Міністерства юстиції від 08.10.98 № 53/5. URL: <https://zakon.rada.gov.ua/laws/show/en/z0705-98#Text>
2. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис....канд. юрид. наук. 12.00.09. Харків, 2017. 22 с. С. 10.
3. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 05 березня 2019 року, судова справа № 202/403/19. URL: <https://reyestr.court.gov.ua/Review/80249913>
4. Ухвала слідчого судді Рівненського міського суду Рівненської області від 02 жовтня 2019 року, судова справа № 569/18629/19. URL: <https://reyestr.court.gov.ua/Review/84709802>
5. Ухвала слідчого судді Галицького районного суду м. Львова від 17 січня 2019 року, судова справа № 461/4904/18. URL: <https://reyestr.court.gov.ua/Review/79240375>
6. Ухвала слідчого судді Кіровоградського районного суду м. Кіровограда від 08 жовтня 2019 року, судова справа № 404/7345/19. URL: <https://reyestr.court.gov.ua/Review/84872136>
7. Ухвала слідчого судді Печерського районного суду м. Києва від 30 травня 2019 року, судова справа № 757/27912/19-к. URL: <https://reyestr.court.gov.ua/Review/82217099>
8. Ухвала слідчого судді Печерського районного суду м. Києва від 30 травня 2019 року, судова справа № 757/27940/19-к. URL: <https://reyestr.court.gov.ua/Review/82217090>

9. Ухвала слідчого судді Ківерцівського районного суду Волинської області від 29 червня 2022 року, судова справа № 158/806/22. URL: <https://reyestr.court.gov.ua/Review/105036977>
10. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 02 листопада 2023 року, судова справа № 202/13474/23. URL: <https://reyestr.court.gov.ua/Review/115016510>
11. Ухвала слідчого судді Індустріального районного суду м. Дніпропетровська від 15 листопада 2023 року, судова справа № 202/13474/23. URL: <https://reyestr.court.gov.ua/Review/115050551>