Для забезпечення правильного збору та збереження опублікованих у мережі Інтернет даних та недопущення втрати такої інформації у зв'язку з її видаленням:

1. *Має бути здійснене повне збереження вебсторінки за допомогою будь-якого браузера (Google chrome, Firefox, Opera та інші).*
2. *Утворюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.*
3. *За допомогою інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та інші), здійснюється архівація потрібної сторінки.*
4. *Уся послідовність дій під час проведення слідчої дії огляду інформації, розміщеної в Інтернеті, підлягає чіткому відображенню у протоколі огляду з графічним копіюванням вебсторінок та збереженням цифрової інформації на диску.*

Важливо наголосити, що цифрова копія такого документа, що буде прирівнюватися до оригіналу, має зберігатися у тому вигляді, в якому вона створювалася. Це означає збереження оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний.

3.2. Способи збирання електронних доказів

КЕЙС 1. ***Проаналізуйте наведену нижче ситуацію та визначте, які необхідно провести процесуальні дії для розслідування цього злочину?***

На початку травня 2021 року, Петренко О. А., діючи з корисливих мотивів, будучи обізнаним про важке матеріальне становище Котіної П. О. з використанням обману і, використовуючи її уразливий стан, запропонував їй через спілкування в соцмережі Instagram виїхати у м. Ерджан Турецької Республіки Північний Кіпр для роботи танцівницею в нічному клубі у вищезазначеному місті, при цьому не вказавши, що їй доведеться надавати сексуальні послуги незнайомим особам. Отримавши від

останньої згоду, Петренко О. А. виконав відведену йому функцію, визначивши час, місце і спосіб виїзду Котіної у м. Ерджан Турецької Республіки Північний Кіпр.
Прибувши до міжнародного аеропорту м. Ерджан Турецької Республіки Північний Кіпр, Котіну зустрів чоловік на ім'я Махмуд, який доставив її до нічного клубу «Шерідан», розташований у м. Ерджан Турецької Республіки Північний Кіпр, де надалі їй довелося надавати сексуальні послуги.
06 червня 2021 року за заявою потерпілої Котіної було розпочато розслідування за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 149 КК України.
Під час допиту потерпіла повідомила, що у неї є номер телефону чоловіка на ім'я Іван (050-721-66-92), а також його електронна адреса – ivan@mail.ru.

КЕЙС 2. ***Проаналізуйте наведену нижче ситуацію та дайте відповідь на запитання:***

1. ***Які судові експертизи підлягатимуть призначенню та проведенню, предметом яких виступатимуть електронні докази, в описаній ситуації?***
2. ***Судовим експертам яких установ такі експертизи можуть бути доручені?***
3. ***Які орієнтовні питання варто поставити експертам для з'ясування фактів та обставин, що мають істотне значення для цього кримінального провадження?***

У ході проведення досудового розслідування у кримінальному провадженні, відомості про яке внесені до Єдиного реєстру досудових розслідувань за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 203-2 КК України (незаконна діяльність з організації або проведення азартних ігор) встановлено, що в одному із приміщень міста, яке належало підозрюваному на праві приватної власності, під прикриттям офіційної діяльності пунктів з розповсюдження державних лотерей, було облаштовано незаконний гральний заклад, в якому, використовуючи комп'ютерну техніку та доступ до мережі Інтернет, клієнтам надавався доступ до азартних ігор.

> *З метою фіксації виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знарядь кримінального правопорушення та майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб, слідчим на підставі ухвали слідчого судді було проведено обшук приміщення грального закладу під назвою «Твоя Лотерея», в ході якого, серед іншого, було виявлено та вилучено наступне: монітори, системні блоки, клавіатури, комп'ютерні миші, роутери, мобільні телефони та грошові кошти.*

Прийняття нового КПК України запровадило шлях до інформатизації кримінального провадження через запровадження складних технічних НСРД спрямованих на отримання значного обсягу електронної інформації. 180

Поява електронної форми фіксації, передачі і використання інформації викликає потребу в розробці нових методів виявлення, фіксації та оцінки доказів під час розслідування кримінальних правопорушень, особливо тих, які вчиняються із використанням засобів комп'ютерної техніки. 181

У більшості випадків розслідування кіберзлочинів відбувається із використанням можливостей оперативно-розшукових заходів та негласних слідчих (розшукових) дій. Не зупиняючись на окремих аспектах оперативно-розшукової протидії кіберзлочинам, розглянемо можливості слідчих (розшукових) дій під час розкриття кіберзлочинів. 182

Практика ВС щодо використання електронного документа як доказу. Варто погодитися з думкою, що під цифровими технологіями в кримінальному процесі можна вважати законодавчо урегульовану єдину систему засобів та прийомів збирання, фіксації, обробки, зберігання та поширення інформації[82] про кримінальне правопорушення з метою 183

[82] *Берназюк О. О.* Цифрові технології у праві: тенденції та перспективи розвитку : дис. ... д-ра юрид. наук: 12.00.07. Ужгород, 2021. С. 422.

одержання доказів у кримінальному провадженні. На підставі цих доказів слідчий, дізнавач, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

184 Відповідно до результатів проведеного Верховним Судом дослідження практики судів першої, апеляційної та касаційної інстанцій щодо справ, які перебували на розгляді у 2018 та 2019 роках, встановлено поширеність подання сторонами електронних доказів у кримінальних провадженнях, що зумовлено особливостями окремих видів злочинів, спосіб вчинення яких безпосередньо передбачає використання тих приладів та пристроїв, які оперують інформацією в електронному (цифровому) вигляді.

185 Унаслідок цього фактичні дані, на підставі яких суд встановлює наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню, існують саме в електронній (цифровій) формі.

186 ВС зазначив, що відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг», у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа.

187 Матеріальний носій – лише спосіб збереження інформації, який має значення, тільки коли електронний документ виступає доказом. Головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення.

188 ВС підкреслив, що долучений в якості речового доказу DVD-R-диск з відеозаписом обставин події був виготовлений у зв'язку із необхідністю надання інформації, яка має значення у кримінальному провадженні, та є самостійним джерелом доказу, похідним від інформації, що зберігається на комп'ютері в електронному вигляді у вигляді файлів.

189 Отже, записаний на оптичний диск – носій інформації, електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа[83].

190 Вказаний підхід був уточнений об'єднаною палатою Верховного Суду, яка зазначила, що ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія.

191 Для виконання завдань кримінального провадження, з огляду на положення Закону України «Про електронні документи та електронний документообіг», допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону, у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той же електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за

[83] Постанова Верховного Суду від 10.09.2020 року у справі № 751/6069/19. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/91722819

допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами – *CRC*-сума, *hash*-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень[84].

192 На розгляді Верховної Ради України до цього часу перебуває законопроєкт, яким пропонується внести відповідні зміни до КПК України, що стосуються:

1) визначення поняття та видів електронних доказів, доповнивши перелік процесуальних джерел доказів, та розмежувавши поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі;
2) регламентації порядку спеціальної конфіскації віртуальних активів[85].

193 Водночас 1 січня 2022 року в Україні набув чинності Закон України «Про електронні комунікації»[86], який замінив собою раніше діючий Закон України «Про телекомунікації»[87]. Новим законом було визначено правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь

---

[84] Постанова Верховного Суду від 29.03.2021 р. у справі № 554/5090/16-к. URL : https://ips.ligazakon.net/document/C017482?an=178

[85] Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : Проєкт Закону України № 4004 від 01.09.2020. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69771&pf35401=533919

[86] Про електронні комунікації : Закон України № 1089-IX від 16 грудня 2020 року [із змінами і доповненнями]. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text

[87] Про телекомунікації : Закон України № 1280-IV від 18 листопада 2003 [із змінами і доповненнями на 23.02.2014]. *Офіційний вісник України*. 2003. № 51. Ст. 2644.

у відповідній діяльності або користуються електронними комунікаційними послугами. Попри те, положеннями зазначеного закону передбачено розмежування даних про рух інформації та безпосередньо інформації, що передається за допомогою електронних комунікацій.

У подальшому Законом України № 2137-IX від 15 березня 194
2022 року «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам»[88] до КПК було внесено хоч і фрагментарні, проте необхідні та загалом позитивні зміни, якими, серед іншого, було запроваджено терміни «комп'ютерні дані», «комп'ютерні системи» у кримінальному провадженні; передбачено нову гласну слідчу (розшукову) дію – зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису; а також змінено найменування та удосконалено правове регулювання процесуального порядку здійснення таких негласних слідчих (розшукових) дій, як зняття інформації з електронних комунікаційних мереж та установлення місцезнаходження радіообладнання (радіоелектронного засобу).

Важливо наголосити, що вагомою складовою успішного 195
результату розслідування кіберзлочинів є оперативність та повнота здобутих джерел доказової інформації[89]. Оскільки будь-

[88] Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України № 2137-IX від 15.03.2022. *Офіційний сайт Верховної ради України*. URL : https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 13.08.2023).

[89] *Теплицький Б. Б.* Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин

який контент сайту (до прикладу, сторінка користувача соціальної мережі) підтримується за допомогою електронно-обчислювальних ресурсів, завжди існує ризик втрати криміналістично значущої інформації, зумовлений такими факторами. По-перше, сервер, за допомогою якого підтримується контент сайту, може бути знищений або з нього повністю або частково буде видалена потрібна інформація. По-друге, інформація, що міститься в контенті сайту, може бути частково або повністю змінена, наприклад, особою, яка має доступ до контенту на правах адміністратора. Отже, якщо не здійснити оперативну фіксацію і вилучення потрібних для розслідування даних з віддалених серверів, то до моменту вилучення цифрових даних вони можуть вже бути видалені або змінені. Через це при розслідуванні кіберзлочинів виникає необхідність із залучення спеціаліста, особливо у тих випадках, коли здійснення слідчих (розшукових) дій потребує негайних рішень та існує ризик знищення слідів злочину[90].

196 **Система процесуальних дій, які використовуються під час розкриття кіберзлочинів.** Можна виокремити систему процесуальних дій, які найчастіше використовуються під час розкриття кіберзлочинів, яка складається з гласних і негласних слідчих (розшукових) дій, а також такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей та документів.

197 Зокрема, до гласних слідчих (розшукових) дій, в ході яких можна отримати електронні докази, належать наступні:

- обшук житла чи іншого володіння особи;
- призначення комп'ютерно-технічної експертизи.

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. С. 182.

[90] *Гребенькова М. С.* Актуальні проблеми електронних відображень у соціальних мережах як джерела доказів у кримінальному провадженні. *Право і суспільство*. 2021. № 6. С. 256.

198 До негласних слідчих (розшукових) дій, у процесі яких можна отримати електронні докази, варто віднести:

- аудіо-, відеоконтроль особи;
- зняття інформації з електронних комунікаційних мереж;
- зняття інформації з електронних інформаційних систем;
- аудіо-, відеоконтроль місця.

199 Також електронні докази можуть отримуватися в ході тимчасового доступу до речей та документів, а також добровільно надаватися учасниками кримінального провадження.

200 **Принципи роботи з цифровою інформацією, що є доказом**. Міжнародною організацією з цифрових доказів (*International Organisation on Digital Evidence* (IOCE)) визначені такі принципи роботи з цифровою інформацією, що є доказом:

1) при роботі з доказовою інформацією, що міститься на цифровому носії, повинні дотримуватися процесуальні і криміналістичні вимоги;
2) при операціях з доказовою інформацією на цифрових носіях неприпустимо внесення змін до цієї інформації;
3) всі операції з виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях повинні бути зафіксовані в документальній формі, захищені від несанкціонованої зміни і придатні для дослідження;
4) особа, яка здійснює операції з доказовою інформацією на цифрових носіях, несе відповідальність за її збереження, поки має доступ до цієї інформації;
5) будь-яка організація, що здійснює виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях, повинна дотримуватися вказаних принципів[91].

[91] Digital Evidence: Standards and Principles. *Forensic Sciennce Communications*. 2000. Vol. 2. № 2. URL : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.

201 **Особливості слідчих (розшукових) та інших процесуальних дій, проведення яких спрямоване на збирання та перевірку електронних доказів**.

202 1. Процесуальна коректність фіксації: зміст і реквізити цифрової інформації підлягають обов'язковому опису в протоколі слідчої дії або експертному висновку. Однак найчастіше виключно документально-текстова фіксація є недостатньою, тому рекомендується вносити в текст процесуального документа або прикладати до нього скріншоти, роздруківки логів, витяги із зовнішньої аналітики та статистики по сайту тощо. У разі копіювання цифрової інформації, також має бути доданий її носій. Окрім того, до участі у слідчому огляді рекомендується залучати понятих, яким потрібно послідовно роз'яснювати сутність усіх дій слідчого та спеціаліста, які мають значення для розслідування.

203 2. Точний опис проведених операцій із виявлення програмного забезпечення (включаючи точну версію), зокрема і використаних для цього технічних засобів. Специфіка подібної вимоги полягає в тому, що на відміну від багатьох інших слідів, цифрова інформація, особливо розміщена в Інтернеті, після вивчення суб'єктом розслідування може залишитися незмінною. Відповідно, комплекс операцій з її виявлення та фіксації повинен становити собою формалізований алгоритм, який при необхідності може бути точно відтворений згодом. Фіксації підлягають не тільки виявлені пристрої, а й навколишнє оточення. Відомості про обстановку дають підстави судити про умови як використання особою, яка вчинила злочин, електронних носіїв інформації, так і умови виявлення та процесуального вилучення цих носіїв.

204 3. Коректність встановлення зв'язку виявленої інформації з подією, що розслідується або особою підозрюваного, у тому числі робота з встановлення або спростування «цифрового

алібі». Якщо для індивідуалізованих комп'ютерних пристроїв (насамперед, особистих смартфонів) зв'язок інформації, що знаходиться на пристрої із власником пристрою може вважатися апріорним, то для стаціонарних пристроїв, особливо які розташовані в місцях, де доступ до них можуть мати різні суб'єкти, потрібне додаткове обґрунтування обумовленості операцій з цифровою інформацією з діями конкретної особи. При цьому дослідники звертають увагу на особливості перевірки такого алібі з урахуванням того, що, по-перше, доказова інформація, яка підтверджує чи спростовує «цифрове алібі», недоступна для безпосереднього сприйняття, і для її вивчення необхідно використовувати програмно-технічні засоби; по-друге, така доказова інформація є вкрай нестійкою, оскільки може бути легко знищена (у тому числі й некваліфікованими діями слідчого)[92].

Розглянемо більш детально процесуальний порядок 205
проведення та особливості кожної із процесуальних дій.

Обшук житла чи іншого володіння особи. В ході обшуку 206
слідчий може вилучати значну кількість носіїв цифрової інформації, яка в подальшому може бути використана як докази у кримінальному провадженні.

Відповідно до ч. 1 ст. 234 КПК України, обшук проводиться 207
з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб.

У клопотанні про обшук, окрім іншого, повинні міститися 208
відомості про індивідуальні або родові ознаки речей, документів,

---

[92] *Цехан Д. М.* Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 257.

іншого майна або осіб, яких планується відшукати, а також їхній зв'язок із вчиненим кримінальним правопорушенням.

209 Базовим завданням цієї слідчої дії є забезпечення безпеки комп'ютерної доказової інформації, а також полегшення її виявлення.

210 Перед обшуком бажано отримати орієнтуючу інформацію щодо комп'ютерної техніки, яка знаходиться на місці обшуку. До таких відомостей можна віднести інформацію про:

- кількість, типи, марку та конфігурацію ЕОМ;
- наявність локальної мережі або підключення комп'ютера до глобальної мережі Internet;
- кваліфікацію користувачів ЕОМ в галузі програмування та обчислювальної техніки;
- факт використання пристрою автономного та безперебійного живлення, і до яких наслідків може призвести вимкнення електроенергії;
- характеристику колективу співробітників, які обслуговують обчислювальну техніку[93].

211 При дослідженні зовнішніх характеристик комп'ютерного пристрою варто звернути увагу й описати в протоколі слідчої дії всі підключені до нього периферійні пристрої вводу-виводу: монітори, клавіатури, комп'ютерні миші та інші маніпулятори, веб-камери, принтери, сканери, копіри, модеми, хаби і т. п. При зовнішньому огляді доцільно шукати можливі відключені накопичувачі інформації. У протоколі повинен також міститися опис усіх підключених кабелів та незайнятих портів. Вкрай бажано сфотографувати розташування та факт підключення кабелів. При вилученні комп'ютерного пристрою, якщо є

[93] *Теплицький Б. Б.* Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. С. 127.

необхідність вимкнення кабелю, необхідно маркувати кожен кабель і відповідний порт, наприклад, за допомогою паперових або пластикових бирок.

Більше того, у протоколі необхідно описати: 212

- найменування, марку та модель комп'ютерного пристрою, місце його виявлення або особу, в якої він був фактично вилучений та за яких обставин;
- ідентифікаційні ознаки, зокрема серійний номер, із зазначенням способу ідентифікації (напис на пристрої, електронна інформація тощо);
- про те, що (у разі вилучення незаблокованого пристрою) на момент вилучення такий пристрій є незаблокований та відобразити здійснені суб'єктом проведення відповідної слідчої (розшукової) дії заходи щодо увімкнення режиму польоту та вимкнення Wi-Fi і Bluetooth;
- перебіг та результати копіювання всього вмісту пристрою, із зазначенням всіх здійснених суб'єктом проведення відповідної слідчої (розшукової) дії заходів, включаючи інформацію, що підлягає копіюванню, програмного забезпечення, за допомогою якого відбувається таке копіювання, відомості про його ліцензування, носій інформації, на який здійснено копіювання наявної на комп'ютерному пристрої інформації, із зазначенням ідентифікаційних номерів носія інформації (серійний чи інвентарний номер тощо)[94].

Вилучені мобільні пристрої (телефони, планшетні 213
комп'ютери, GPS-навігатори, *smart*-годинники, портативні відеореєстратори тощо) упаковуються в окремі непрозорі

[94] Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 43.

пакети, що унеможливлює увімкнення пристрою в упаковці[95].

214 Отже, в протоколі обшуку повинно бути детально зазначено всі можливі ідентифікаційні ознаки об'єктів комп'ютерної техніки. Згідно з правовою позицією Верховного суду, протокол обшуку, в якому відсутні ідентифікаційні ознаки виявлених та вилучених речей (не зазначено марки, моделі, номера, а також характерних ознак), є недопустимим доказом[96].

215 Слідчий, прокурор під час проведення обшуку має проаналізувати обстановку й обрати найбільш прийнятний (процесуально допустимий) спосіб отримання інформації: вилучати електронні носії інформації або копіювати інформацію, що міститься в інформаційній системі. Для прийняття зваженого рішення варто використовувати наступний ***алгоритм*** (див. схему 1)[97].

216 Важливим елементом процесу аналізу обстановки на місці проведення обшуку, огляду є можливість проведення експрес-пошуку інформації як форми огляду документів під час обшуку, огляду, що передбачено ч. 7 ст. 236 КПК України. Важливо зауважити, що експрес-пошук не дозволяє проаналізувати значну частину видалених файлів, а також зашифровані та заблоковані дані, однак така дія надає можливість визначитися з наступними рішеннями при проведенні обшуку, огляду.

---

[95] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 46.

[96] Постанова Верховного суду від 24.09.2020 р. у справі №306/2629/17. URL : https://ips.ligazakon.net/document/c015095?an=2

[97] *Гаркуша А., Каланча І.* Як вилучати електронні носії інформації під час обшуку з користю для слідства і без шкоди для бізнесу. алгоритм прийняття рішень. URL : https://justtalk.com.ua/post/yak-viluchati-elektronni-nosii-informatsii-pid-chas-obshuku-z-koristyu-dlya-slidstva-i-bez-shkodi-dlya-biznesu-algoritm-prijnyattya-rishen

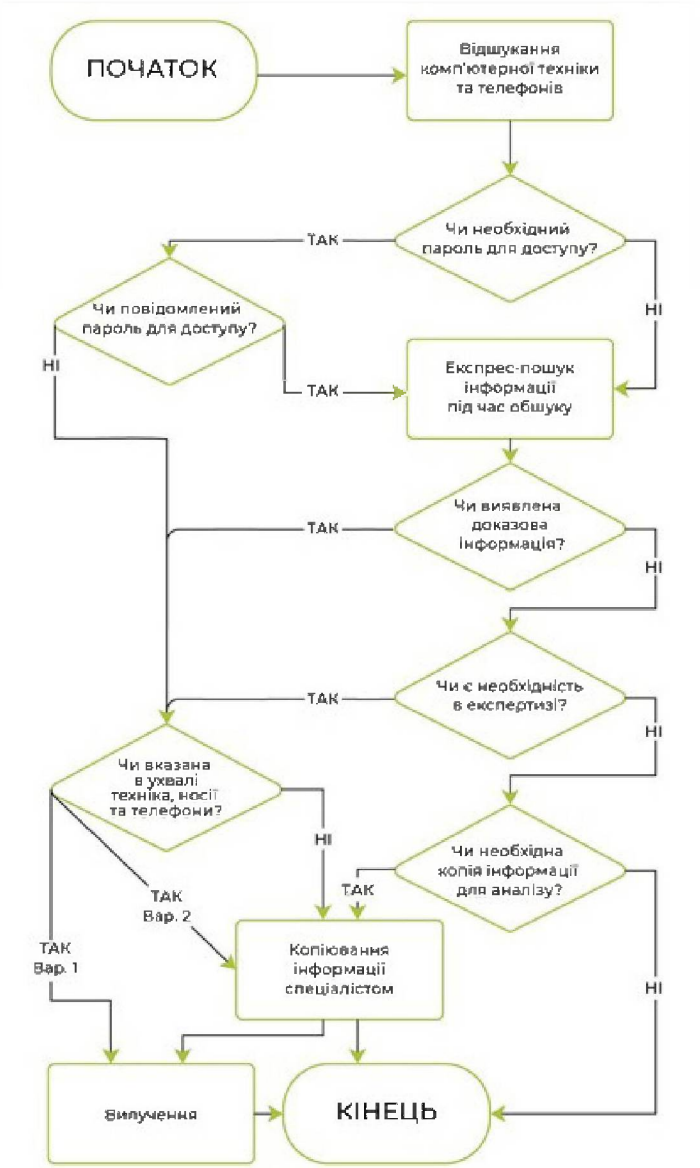

ПОЧАТОК
Відшукання комп'ютерної техніки та телефонів
Чи необхідний пароль для доступу?
ТАК
НІ
Чи повідомлений пароль для доступу?
НІ
ТАК
Експрес-пошук інформації під час обшуку
Чи виявлена доказова інформація?
ТАК
НІ
Чи є необхідність в експертизі?
ТАК
НІ
Чи вказана в ухвалі техніка, носії та телефони?
НІ
ТАК Вар. 2
ТАК Вар. 1
Чи необхідна копія інформації для аналізу?
ТАК
НІ
Копіювання інформації спеціалістом
Вилучення
КІНЕЦЬ

Схема 1

217 Не менш важливою є процедура копіювання електронної інформації, що визначена в абз. 4 ч. 2 ст. 168 КПК України. Це ефективний спосіб отримання доказової інформації, що може бути надалі дієво використаний слідчим та прокурором з огляду на статус такої інформації як оригінала документа (ч. 4 ст. 99 КПК України).

218 *Технічна неможливість копіювання електронної інформації є достатнім обґрунтуванням необхідності подальшого експертного дослідження.* Варто додати, що у випадку, коли з технічних причин неможливо скопіювати електронну інформацію з об'єктів, що не вказані в ухвалі слідчого судді, слідчий, прокурор можуть їх тимчасово вилучити в порядку, визначеному ч. 7 ст. 236 КПК України (як речі, що мають важливе значення для кримінального провадження). При цьому у протоколі мають бути зафіксовані виявлені відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження, а метою вилучення, за таких умов, є забезпечення збереження цілісності інформації на електронному носії, а не вивчення фізичних властивостей, оскільки такі властивості в достатньому обсязі вивчені до ухвалення рішення про вилучення носія (абз. 2 ч. 2 ст. 168 КПК України)[98].

219 **Призначення та проведення комп'ютерно-технічної експертизи.** Комп'ютерно-технічна судова експертиза (далі – КТЕ), становить самостійний вид судових експертиз, що належить до класу інженерно-технічних, її проводять з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення

[98] *Гаркуша А., Каланча І.* Як вилучати електронні носії інформації під час обшуку з користю для слідства і без шкоди для бізнесу. Алгоритм прийняття рішень. URL : https://justtalk.com.ua/post/yak-viluchati-elektronni-nosii-informatsii-pid-chas-obshuku-z-koristyu-dlya-slidstva-i-bez-shkodi-dlya-biznesu-algoritm-prijnyattya-rishen

й вивчення його слідової картини в розслідуваному злочині, а також одержання доступу до інформації на носіях даних з подальшим усебічним її дослідженням. Тільки КТЕ спроможна, забезпечивши отримання органами досудового розслідування унікальної розшукової інформації, створити відповідно до норм КПК України процесуальне джерело доказів – висновок експерта. За таких умов невідкладними й найважливішими завданнями слідчих та оперативних працівників є пошук, фіксація, вилучення й надання експерту в непошкодженому вигляді матеріальних об'єктів – носіїв комп'ютерної інформації, що набувають статусу об'єктів експертного дослідження, і правильне визначення завдань КТЕ[99].

Систему об'єктів КТЕ становлять класи (які поділяють на 220
види й підвиди), а саме:

апаратних об'єктів:

- персональні комп'ютери (у будь-яких варіантах виконання);
- периферійні пристрої до персональних комп'ютерів;
- мережеві апаратні засоби (сервери, робочі станції, комутатори, модеми, роутери й інше серверне обладнання);
- інтегровані системи (мобільні телефони тощо);
- будь-які комплектувальні всіх зазначених вище компонентів (апаратні блоки, блоки живлення, плати розширення тощо).

Ці види можуть поєднуватися. Безпосередньо в контексті 221
криміналістики найважливіший підвид запам'ятовувальних пристроїв та інших носіїв інформації (електронних даних) – усі відомі на момент призначення експертного дослідження носії інформації (електронних даних): жорсткі диски, флеш-

[99] *Теплицький Б. Б.* Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2. С. 25.

накопичувачі, диски для лазерних систем зчитування, карти пам'яті тощо. До апаратних об'єктів належать: системний блок; жорсткий диск; інші накопичувачі даних – гнучкі диски (5.25» і 3,5»), CD-ROM, магнітооптичні диски; сервер (на платформі Intel-процесорів або сумісних із ними); *RAID*-масиви; принтери (під час виконання комплексної експертизи разом із технічною експертизою документів);

222 *програмних об'єктів:*

- системне програмне забезпечення – комплекс програм, призначених для управління роботою обчислювальної системи, розподілу її ресурсів, підтримання діалогу з користувачами, надання їм допомоги в обслуговуванні комп'ютера, а також для часткової автоматизації розроблення нових програм. Системне програмне забезпечення поділяють на три основні складові: операційні системи, системи програмування, сервісні програми;
- прикладне програмне забезпечення – комплекс програм, призначених для виконання прикладних завдань фахової діяльності людини (виробничі, наукові, навчальні, розважальні тощо);

223 *інформаційних об'єктів (електронних даних):*

- текстові й графічні файли, створені з використанням комп'ютерів або мобільних пристроїв;
- аудіовізуальні (мультимедійні) дані;
- інформація у форматах баз даних та іншого прикладного програмного забезпечення[100].

224 Повноцінна організація проведення КТЕ передбачає наявність спеціалістів з різних операційних систем, прикладного

[100] *Теплицький Б. Б.* Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ.* 2019. № 2. С. 26.

програмного забезпечення, бухгалтерських програм, баз даних, програмування, криптоаналізу, мультимедіа, мережевих та інтернет-технологій, апаратних компонентів комп'ютера та машинних носіїв інформації, зв'язку.

Можна виокремити такі завдання, які вирішуються під час 225
проведення КТЕ:

- визначення робочого стану комп'ютерно-технічних засобів, а також властивостей, якості, статусу та особливостей використання технічних комп'ютерних систем;
- встановлення особливостей розробки і використання програмних продуктів (при встановленні фактів використання програмного забезпечення з порушенням авторських прав його розробника);
- установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;
- виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;
- встановлення вартості програмного забезпечення;
- отримання доступу до інформації на носіях;
- підтвердження або спростування заявлених розробником характеристик, алгоритмів та властивостей програмного забезпечення;
- дослідження інформації, створеної користувачем або програмою для реалізації інформаційних процесів;
- виявлення причин блокування сайтів (віруси, мережеві атаки), а також несанкціонованого втручання в роботу сайту, сервера, комп'ютера, електронної пошти тощо;
- ідентифікаційне дослідження мережевих комунікацій та інтернет-технологій[101].

[101] *Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В.* Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посібник. Львів : Львівський державний університет внутрішніх справ, 2022. С. 36–37.

226 Окрім типових задач, у практиці цього роду експертиз трапляються й нестандартні задачі, що потребують використання спеціальних методичних підходів. До них належать, наприклад, дослідження апаратних засобів за наявності комплексу несправностей або ж дослідження несправностей апаратних засобів, що викликані зовнішнім впливом (механічним та термічним), а також впливом водяного потоку (залив). До цієї ж категорії належать і задачі диференціації електронних інформаційних пристроїв, які відносять (або не відносяться) до класу комп'ютерів. Останнім часом до цієї групи входить і встановлення комп'ютерної імітації (використання комп'ютерних систем для виготовлення грошей, зображень відбитків печаток і штампів тощо), що потребує комплексного підходу при дослідженні[102].

227 **Аудіо-, відеоконтроль особи.** Одним із різновидів втручання у приватне спілкування згідно з ч. 4 ст. 258, ст. 260 КПК є аудіо-, відеоконтроль особи, який є НСРД, що проводиться без відома такої особи на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування. Зазначену НСРД законодавець розмістив першою серед негласних засобів отримання інформації, у такий спосіб визначивши її важливе значення у досудовому розслідуванні злочинів[103]. Водночас обмеженість правового регулювання та

[102] *Карпінська Н., Крикунов О.* Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис.* 2017. № 1. С. 142.

[103] Окрім того, варто зазначити, що за матеріалами узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії, у провадженні апеляційних судів перебувало 10,9 тис. клопотань про аудіо-, відеоконтроль особи, з яких задоволено 9,9 тис. (Див.: Постанова Пленуму Вищого спеціалізованого суду

невизначеність співвідношення із суміжними негласними діями визначає необхідність у її науковому осмисленні та узагальненні практики проведення.

У п.п. 1.11.2. Інструкції вказано, що ця НСРД полягає у 228
негласній (без відома особи) фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування тощо. На думку Ю. Лисюка метою аудіоконтролю є спостереження за діями та розмовами особи (шляхом прослуховування та фіксації розмов) у будь-якому місці її перебування, незважаючи на те, що це місце є її власністю чи вона там тимчасово перебуває, а відеоконтролю – візуальне негласне спостереження за діями особи (шляхом відеозапису та аудіофіксації) у будь-якому місці її перебування для отримання інформації, що має значення для досудового розслідування[104]. С. Єськов уважає, що метою зазначеної НСРД є фіксація з використанням аудіо-, відеозаписуючих пристроїв поведінки особи, її розмов або інших рухів, дій, пов'язаних із її діяльністю або місцем перебування у публічно недоступних місцях[105]. Погоджуючись із зазначеними вченими, варто додати, що метою усіх НСРД є пошук та фіксація відповідних відомостей, які у перспективі матимуть доказове значення, проте більшість із таких дій мають власну

України з розгляду цивільних і кримінальних справ № 3 від 07 лютого 2014 року «Про узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії». URL : http://zakon3.rada.gov.ua/laws/show/v0003740-14

[104] *Лисюк Ю. В.* Аудіо-, відеоконтроль як різновид втручання у приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Науковий вісник Херсонського державного університету.* 2014. Вип. 6-1. Т. 4. С. 79.

[105] *Єськов С. В.* Аудіо-, відеоконтроль особи як різновид втручання у приватне спілкування : системно-структурний аналіз. URL : www.corp-lguvd.lg.ua/d130203.html

спрямованість, що обумовлює виокремлення їх у відповідний вид (класифікацію).

229 Щодо аудіо-, відеоконтролю особи, то аналіз глави 21 КПК дає змогу припустити, що ще дві НСРД мають аналогічну мету та об'єкти проведення. Йдеться про спостереження за особою, місцем або річчю та аудіо-, відеоконтроль місця. Об'єктом аудіо-, відеоконтролю особи є приватне спілкування особи у публічно недоступних місцях у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, зміст яких має значення для досудового розслідування. Такі ж об'єкти передбачені і щодо названих вище НСРД, відмінність лише щодо публічності (доступність чи недоступність) місця проведення та особливостей організаційно-тактичного та технічного забезпечення. Тому, погоджуємося з В. Уваровим у тому, що усі три НСРД мають однакові об'єкти, предмети і методи дослідження. Вони мають своїм змістом спостереження за особою й окремими місцями її перебування та різняться хіба що рівнем їх технологізації[106]. В. Тертишник зазначає, що такі НСРД, як аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця та спостереження за особою, річчю або місцем часто мають або один метод, або один предмет дослідження та перебувають у стані штучної конкуренції правових норм. На його думку, наведені вище НСРД можуть і мають бути об'єднані в єдину слідчу дію – візуальне спостереження та технічне документування, порядок провадження якої, як наголошує вчений, має бути ретельно прописаним у законі[107].

230 Аудіоконтроль особи полягає у прослуховуванні та фіксації розмов, що відбуваються на відповідних об'єктах. Аудіоконтроль

---

[106] *Уваров В. Г.* Інститут втручання у приватне життя шляхом аудіо-, відео контролюю. *Право і безпека.* 2012. № 5 (47). С. 191.

[107] *Тертишник В. М.* Концептуальні проблеми реформи кримінального судочинства *Право і суспільство.* 2013. № 1. С. 139.

особи проводиться за допомогою спеціальних технічних засобів фіксації інформації. Безпосередній порядок проведення такої НСРД визначається відповідними відомчими нормативно-правовими актами. Аудіоконтроль особи може здійснюватися епізодично (наприклад, на певний проміжок часу проведення зустрічі) та неперервно (на весь проміжок часу проведення цієї дії, визначений в ухвалі слідчого судді).

231 Відеоконтроль особи здійснюється технічними засобами, що забезпечують негласне візуальне спостереження за діями, розмовами, поведінкою підозрюваного, обвинуваченого та осіб, що контактують з ними у зв'язку з їх протиправною діяльністю. Відеоконтроль обстановки та дії осіб, їх фіксація може відбуватися в житлі або іншому володінні особи, а також у приміщеннях, транспортних засобах та інших місцях, які не належать до житла та не є іншим володінням особи. Відеоконтроль особи, як правило, здійснюється спеціальними підрозділами, що забезпечують впровадження та експлуатацію СТЗ. Посадова особа уповноваженого оперативного підрозділу правоохоронного органу, якій було доручено аудіо-, відеоконтроль особи, негайно після завершення цієї НСРД повідомляє про це слідчого та надає йому для дослідження інформацію, отриману при застосуванні технічних засобів. Слідчий, а в разі необхідності спеціаліст відповідно до вимог ст. 266 КПК вивчає зміст отриманої інформації, про що складає протокол.

232 Процесуальний порядок проведення аудіо-, відеоконтролю особи є загальним, і передбачає постановлення ухвали слідчим суддею на підставі клопотання слідчого (погодженого з прокурором) або прокурора.

233 За результатами проведення аудіо-, відеоконтролю особи складається протокол, в якому описуються технічні носії інформації, технічні засоби, за допомогою яких була відтворена

наявна в них інформація, результати дослідження наданої інформації. У ньому повністю відтворюється інформація із зазначенням змісту розмови осіб або інших звуків, рухів, дій, пов'язаних з її діяльністю. Протокол про проведення дослідження інформації, отриманої при застосуванні технічних засобів, не пізніше, ніж через двадцять чотири години з моменту припинення аудіо-, відеоконтролю особи передається прокурору (ч. 3 ст. 252 КПК).

234 Проведенню аудіо-, відеоконтролю особи завжди передує обстеження публічно недоступних місць, житла чи іншого володіння особи, в результаті таємного проникнення до яких встановлюються технічні засоби аудіо-, відеоконтролю особи (п. 5 ч. 1 ст. 267 КПК). Тому в разі отримання відомостей слідчим, прокурором, які мають значення для кримінального провадження про розмови конкретної особи або інші звуки, рухи, дії, пов'язані з її діяльністю та перебуванням всередині публічно недоступних місць, житла чи іншого володіння особи, вони звертаються з клопотанням до слідчого судді про дозвіл на проведення обстеження публічно недоступних місць, житла чи іншого володіння особи для встановлення технічних засобів аудіо-, відеоконтролю особи та про дозвіл на проведення аудіо-, відеоконтролю особи всередині цих місць. Як зазначають деякі дослідники, аудіо-, відеоконтроль особи часто проводиться одночасно зі спеціальним слідчим експериментом щодо службової особи під час її зустрічі з особою, що буде надавати неправомірну вигоду, у публічно недоступному місці[108].

235 **Зняття інформації з електронних комунікаційних мереж.** Зняття інформації з електронних комунікаційних мереж полягає в негласному проведенні із застосуванням відповідних

[108] *Шумейко Д. О.* Негласний елемент у системі тактичної операції по документуванню прийняття пропозиції (обіцянки) та одержання неправомірної вигоди. *Наше право*. 2015. № 3. С. 106.

технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду).

Відповідно до ст. 1 ЗУ «Про електронні комунікації», 236
електронна комунікаційна мережа – це комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг. Така мережа – це основна частина інфраструктури будь-якого оператора телекомунікації, чи то оператора традиційної телефонії, стільникового оператора, провайдера безпровідного або провідного доступу до Інтернету[109].

При цьому постачальники електронних комунікаційних 237
мереж та/або послуг зобов'язані вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж (ч. 2 ст. 119 Закону України «Про електронні комунікації»).

Інформація, яка зосереджена в пам'яті комплексно- 238
програмного устаткування постачальників електронних комунікаційних послуг, 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 2 ч. 8 ст. 105 Закону «Про електронні комунікації», постачальники електронних

[109] Кримінальний процесуальний кодекс України. Науково-практичний коментар / за ред. Гончаренка В. Г., Нора В. Т., Шумила М. Є. Київ : Юстиніан, 2012. С. 580.

комунікаційних послуг повинні зберігати записи про надані електронні комунікаційні послуги протягом строку позовної давності, визначеного законом.

239 З огляду на положення ст. 119 Закону України «Про електронні комунікації», постачальники електронних комунікаційних послуг повинні забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, отриманих при укладенні договору про надання електронних комунікаційних послуг та наданні електронних комунікаційних послуг. Своєю чергою інформація про електронні комунікаційні послуги, отримані кінцевим користувачем, може надаватися за наявності його попередньої згоди, вираженої у письмовій чи будь-якій іншій формі, що дає змогу зробити висновок про факт надання такої згоди або у порядку та відповідно до вимог Конституції України та законів України.

240 Водночас, ст. 121 згаданого вище нормативно-правового акту передбачено певні умови надання доступу до інформації у передбачених законом випадках:

241 *По-перше,* доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, відбувається виключно на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом.

242 *По-друге,* зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством.

243 *По-третє,* постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість

підключення технічних засобів, зазначених вище, в точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг.

Так, за допомогою додаткових програмно-апаратних 244
комплексів, встановлених на платформі оператора, можлива постановка на відстеження зразка голосу конкретної особи із встановленням IMEI-номера терміналу, номера абонента у разі, якщо така особа починає сеанс голосового зв'язку. Відповідно, можливо проводити запис розмов цієї особи незалежно від того, яким терміналом або абонентським номером вона користується[110].

Через комплексно-програмні пристрої постачальників 245
електронних комунікаційних послуг проходить потік інформації, частина якої залишається в пам'яті для технологічних цілей (статична), а інша частина проходить як наскрізна – динамічна інформація, що в інтересах слідства може бути перехоплена лише на підставі ухвали слідчого судді апеляційного суду. До статичної інформації тимчасовий доступ можливий на підставі ухвали слідчого судді місцевого суду після розгляду клопотання прокурора або слідчого[111].

Як випливає з п.п. 1.11.5.1. Інструкції, зняття інформації з 246
електронних комунікаційних мереж поділяється на два види:

– контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на

[110] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 19.

[111] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства*. 2013. № 4. С. 98.

електронних комунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний 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 електронних комунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

247 Тож, об'єктом першого виду зняття інформації з електронних комунікаційних мереж будуть: телефонні лінії загального користування; відомчі мережі, що мають вихід на телефоні лінії загального користування; виділені мережі зв'язку невиробничого призначення; мережі пересувного радіотелефонного зв'язку; системи пересувного супутникового зв'язку.

248 Різновидом електронної комунікаційної мережі в цьому випадку виступає мережа мобільного зв'язку, яка становить собою рознесені в просторі приймачі, що працюють в одному і тому ж частотному діапазоні, і комутуюче обладнання, що дозволяє визначати поточне місце розташування рухомих абонентів і забезпечувати безперервність зв'язку при переміщенні абонента із зони дії одного приймача в зону дії іншого. Мобільні мережі різних операторів з'єднані одна з одною, а також зі стаціонарною телефонною мережею. Це дозволяє абонентам одного оператора робити дзвінки абонентам іншого оператора, з мобільних телефонів на стаціонарні і зі стаціонарних на мобільні. Крім того, оператори мобільного зв'язку активно укладають між собою договори роумінгу,

завдяки яким абонент, перебуваючи поза зоною покриття своєї мережі, може здійснювати і приймати дзвінки через мережу іншого оператора.

Тож, основними складовими мережі виступають базові 249
станції (мобільні вишки) і мобільні телефони (кінцеве обладнання). Базова станція – це комплекс радіопередавачів (ретранслятори, прийомо-передавачі), який здійснює зв'язок з кінцевим абонентським обладнанням – мобільним телефоном. Зона покриття від антен базової станції утворює соту, або групу сот. Базова станція забезпечує централізоване обслуговування групи кінцевих абонентських пристроїв. Мобільні телефони є кінцевим обладнанням, безпосередньо з якого і ведуться переговори[112].

Зняття інформації з електронних комунікаційних мереж 250
цього виду завжди повинно передбачати контроль розмов обидвох абонентів, шляхом використання безпосереднього підключення до телефонного каналу або сканування радіоканалу. Прослуховування телефонної розмови тільки одного з абонентів, в тому числі і з використанням технічних засобів, без підключення до мережі зв'язку не вважається зняттям інформації з електронних комунікаційних мереж, а повинно розглядатись, як інша НСРД пов'язана із втручанням у приватне спілкування (наприклад, аудіо-, відеоконтроль особи).

Об'єктом другого виду зняття інформації з електронних 251
комунікаційних мереж будуть: телексні, факсимільні, селекторні, радіорелейні, пейджингові канали обміну інформації між абонентами, комп'ютерні мережі різного рівня.

Фіксація повідомлень, переданих у комп'ютерних мережах, 252
має певні особливості. Загальним правилом є те, що інтернет-

[112] *Багрій М. В., Луцик В. В.* Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід: монографія. Харків : Право, 2017. С. 142.

провайдер, укладаючи договір з користувачем про підключення до глобальної мережі Інтернет, з'ясовує і фіксує в договорі анкетні дані і точну адресу користувача. Це дає можливість «прив'язати» MAC-адресу та IP-адресу комп'ютера до конкретної особи. Однак при реєстрації в чатах, на форумах, у блогах, соціальних мережах користувач може не вказувати свої анкетні дані, а використовувати нікнейм, який становить собою умовне ім'я, яке не містить ніяких реальних відомостей про певну фізичну особу.

253 Всі повідомлення користувача надходять на центральний пристрій – сервер, потім за допомогою інших пристроїв (комутатора, маршрутизатора) направляються абонентам. При цьому відомості про відправника фіксуються і зберігаються на сервері провайдера.

254 Таким способом, повідомлення в комп'ютерних мережах можна відстежити за:

а) MAC-адресою, тобто ідентифікаційною адресою комп'ютерного обладнання;

б) IP-адресою, присвоєною комп'ютеру у відповідній комп'ютерній мережі;

в) адресою електронної поштової скриньки;

г) ідентифікаційному номеру UIN, наявного у користувачів ICQ;

д) даними, що містяться в обліковому записі відвідувачів чатів, форумів, блогів, соціальних мереж.

255 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, електронну комунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування.

До таких ідентифікаційних ознак можна віднести: 256

- електронний код (ідентифікатор) кінцевого обладнання – код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо)[113];
- ідентифікаційна телекомунікаційна картка (далі – ідентифікаційна картка) – засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в електронній комунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо);
- мережевий ідентифікатор споживача – індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в електронній комунікаційній мережі чи Інтернеті. Під ним потрібно розуміти або номер абонента в мережах GSM, CDMA або IP-адресу електронної інформаційної системи (ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад, Інтернет));
- MAC-адреса (*Media Access Control* – управління доступом до носія) – унікальний ідентифікатор, що зіставляється з різними типами обладнання для комп'ютерних мереж (мережевими картами, Wi-Fi роутерами тощо). Усі комп'ютери, підключені до локальної мережі з виходом в Інтернет, як правило, мають дві адреси: логічну адресу мережевого рівня (IP-адресу) і фізичну адресу мережевої інтерфейсної карти (MAC-адресу).

[113] П. 3 Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України № 295 від 11 квітня 2012 р.: [із змінами і доповненнями на 08.04.2013] *Офіційний вісник України*. 2012. № 29. Ст. 1074.

257 Не можна погодитися з думкою, що на сьогоднішній день у слідчого, прокурора чи оперативних підрозділів відсутні практичні можливості надати слідчому судді відомості, які унікально ідентифікують абонента спостереження, адже відсутні документальні підтвердження факту користування конкретною особою кінцевим обладнанням (мобільним телефоном)[114]. Варто зауважити, що закон вимагає від слідчого, прокурора вказати ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження або кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування. Тож, навіть у випадку відсутності договору з оператором мобільного зв'язку конкретної фізичної особи, органи досудового розслідування мають право надавати інформацію, яка ідентифікує кінцеве обладнання, а не абонента.

258 Проведення зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. Керівники та працівники операторів електронних комунікацій зобов'язані сприяти виконанню дій із зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді.

259 За результатами проведення цієї НСРД складається протокол, у якому вказують дату його складення, посаду,

---

[114] *Самбор М. А.* Негласні слідчі (розшукові) дії, пов'язані із зняттям інформації з транспортних телекомунікаційних мереж та встановленням місцезнаходження радіоелектронного засобу: підстави для проведення та умови гарантування прав і свобод людини та громадянина як споживача послуг рухомого (мобільного) зв'язку. *Вісник Дніпропетровського університету ім. А. Нобеля*. 2013. № 1. С. 78. (Серія «Юридичні науки»).

прізвище та ініціали особи, що здійснює кримінальне провадження, номер кримінального провадження у ЄРДР, номер відповідної ухвали, а також дату її прийняття та найменування суду, слідчим суддею якого надано дозвіл на зняття інформації з електронних комунікаційних мереж та строки його здійснення. Окрім того, у протоколі зазначають найменування підрозділу, працівники якого залучалися до здійснення зняття інформації з електронних комунікаційних мереж, дані про особу, стосовно якої здійснювалася НСРД, її результати, відомості про МНІ (матеріали аудіо- чи відеозапису, фото- і кінозйомки, магнітні накопичувачі тощо)[115].

260 Окрім складання цього протоколу ст. 265 КПК визначає, що зміст інформації, яка передається особами через електронні комунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення зняття інформації з електронних комунікаційних мереж. При виявленні в інформації відомостей, що мають значення для конкретного досудового розслідування, в протоколі відтворюється відповідна частина такої інформації, після чого прокурор вживає заходів для збереження знятої інформації. Своєю чергою зміст інформації, одержаної внаслідок здійснення зняття інформації з електронних комунікаційних мереж, фіксується на відповідному носієві особою, яка здійснювала зняття та зобов'язана забезпечити обробку, збереження або передання інформації.

261 Отримана у такий спосіб звукова інформація має бути розшифрована уповноваженою службовою особою із залученням, у необхідних випадках, відповідного спеціаліста. До протоколу цієї НСРД вносяться лише ті фрагменти, які мають значення для

[115] Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1/ за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. С. 668.

кримінального провадження. Як спеціалісти у цьому випадку можуть залучатися фахівці у галузі економіки, кредитування, аграрного сектору, природних ресурсів тощо, залежно від виду розслідуваного кримінального правопорушення. Якщо особи, чия звукова інформація знята з електронних комунікаційних мереж, спілкувалися іноземною мовою, для розшифровування (перекладу) інформації залучають перекладача. Носії інформації, на яких міститься звукозапис розмов, можуть бути досліджені на предмет ототожнення особи за фізичними параметрами голосу та встановлення технічних умов і технології отримання відео-, звукозапису[116].

262 Протоколи про проведення зняття інформації з електронних комунікаційних мереж з додатками не пізніше ніж через двадцять чотири години з моменту припинення вказаних НСРД передають прокурору (ч. 3 ст. 252 КПК).

263 Забороняється використання відомостей, речей та документів, отриманих у результаті проведення НСРД для цілей, не пов'язаних із кримінальним провадженням, або ознайомлення з ними учасників кримінального провадження чи будь-яких інших осіб. Якщо протоколи про проведення НСРД, зокрема зняття інформації з електронних комунікаційних мереж, містять інформацію щодо приватного (особистого чи сімейного) життя інших осіб, захисник, а також інші особи, які мають право на ознайомлення з протоколами, попереджаються про кримінальну відповідальність за розголошення отриманої інформації щодо інших осіб.

---

[116] Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: [навч.-практ. посібник] / Б. І. Бараненко, О. В. Бочковий, К. А. Гусєва та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка. 2014. С. 210.

264 Потрібно враховувати, що МНІ, на яких зафіксовано телефонні розмови осіб, є речовими доказами особливого виду – похідними від усного спілкування. Тому, враховуючи принцип безпосередності дослідження доказів і для перевірки обставин отримання звукозапису, необхідно отримати також показання хоча б однієї з осіб, яка брала участь у телефонній розмові, якщо це можливо. В іншому випадку для перевірки достовірності звукозапису та ідентифікації осіб, які спілкувалися між собою, може бути призначена фоноскопічна (фонографічна) експертиза, яка може дати відповіді на такі питання: Кому з-поміж перелічених осіб належать окремі вислови, що містяться на фонограмі?; Чи є голос, зафіксований на фонограмі, голосом конкретної особи?; Чи зазнавала змін ця фонограма?; Чи наявні ознаки монтажу фонограми?; Які є ознаки механічного та електронного монтажу фонограми?; Чи велась зафіксована на фонограмі розмова по телефону? тощо.

265 Складнощі виникають з матеріалами звукозапису, виготовлених з використанням цифрової техніки. Експерти досі не мають технічної можливості встановити наявність або відсутність ознак монтажу. Якщо експерти роблять висновок про те, що встановити наявність або відсутність ознак монтажу неможливо, зафіксовані на відповідному носії дані стають сумнівними[117].

266 У пам'яті обладнання постачальників електронних комунікаційних послуг часто залишаються дані (SMS, MMS, *e-mail* та інші повідомлення) з текстовою, а також фото-, відеоінформацією, що передається як кореспонденція між особами. Проте варто врахувати, що повідомлення, які надійшли на пошту електронної адреси, SMS, MMS та ін., у тому числі й голосова пошта, повідомлення на автовідповідач, але не відкриті

[117] *Уваров В. Г.* Зняття інформації з технічних каналів зв'язку. *Зовнішня торгівля: економіка, фінанси, право.* 2013. № 2. С. 180.

для прочитування (прослуховування, перегляду), належать до категорії кореспонденції, що охоплюється ст. 8 ЄКПЛ, і доступ до них може бути здійснено лише на підставі статей 261, 263 КПК. Але якщо буде встановлено, що отримувач ознайомлений з їхнім змістом, то вони можуть бути доступними для вилучення в порядку норм глави 15 КПК[118].

267 Окрім того, потрібно враховувати випадки, що навіть, якщо здійснюється онлайн-трансляція, яка є предметом зняття інформації з електронних комунікаційних мереж, то в ході її проведення все одно одержуються цифрові докази. Такий підхід також використовує Верховний Суд, який зазначає, що оскільки зображення через веб-камеру одного комп'ютера транслюється на монітор іншого комп'ютера в системі загальної для них мережі, за час проходження через останню має місце запізнення сигналу з тимчасовим збереженням зображення на серверах та у пам'яті електронних пристроїв для здійснення безперервного потоку інформації шляхом буферизації та створення тимчасових файлів, то фактично наявна форма його матеріальної фіксації в комп'ютерній мережі, в якій відбувається трансляція, хоча і на дуже незначний час[119].

268 **Зняття інформації з електронних інформаційних систем.** Відповідно до п. 1.11.6. Інструкції – зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

---

[118] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства*. 2013. № 4. С. 105.

[119] Постанова Верховного суду від 18.06.2020 року у справі № 711/7900/17. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/89929158

З таким визначенням можна погодитися лише частково, 269
оскільки одержання інформації, що міститься в комп'ютерній мережі за загальним правилом повинно охоплюватись такою НСРД, як зняття інформації з електронних комунікаційних мереж. Отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в тому випадку, коли жоден із елементів локальної мережі не під'єднаний до глобальної мережі.

Електронно-обчислювальна машина (ЕОМ, комп'ютер) являє 270
собою сукупність технічних засобів та системного програмного забезпечення, створює можливість автоматизованого оброблення інформації та отримання результату в необхідній формі. Крім того, відповідно до державних стандартів, комп'ютер – це функціональний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв й може виконувати обчислення без участі людини. Комп'ютер, призначений для обслуговування одного користувача, що характеризується невеликими габаритами, підвищеною надійністю, простотою зміни конфігурації та розвинутими засобами діалогу, є персональним комп'ютером.

Автоматизованою є система, що здійснює автоматизовану 271
обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

Комп'ютерна (інформаційна) мережа – це сукупність 272
територіально розосереджених систем оброблення даних, засобів та/або систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів.

Мережа електрозв'язку являє собою комплекс технічних 273
засобів електронних комунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання

знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, провідних, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

274 Відповідно до ст. 1 ЗУ «Про захист інформації в інформаційно-комунікаційних системах», інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів[120].

275 Зняття інформації з електронних інформаційних систем або їх частин може відбуватися як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення. Негласне зняття інформації із засобів електронно-обчислювальної техніки полягає у застосуванні засобів спеціальної техніки із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диска (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого, що можуть містити інформацію, яка має значення у кримінальному провадженні. Програмне проникнення до електронних інформаційних систем (їх частин) відбувається шляхом застосування спеціальних програмних продуктів, які забезпечують копіювання інформації, що обробляється на ПЕОМ підозрюваного, обвинуваченого, на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю негласну слідчу (розшукову) дію[121].

---

[120] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 : [із змінами і доповненнями на 01.07.2022]. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

[121] Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1/ за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. С. 670–671.

У клопотанні на отримання дозволу на зняття інформації з електронних інформаційних систем слідчий або прокурор повинні зазначити такі відомості: найменування кримінального провадження та його реєстраційний номер; короткий виклад обставин злочину, у зв'язку з розслідуванням якого подається клопотання; правова кваліфікація злочину із зазначенням статті (частини статті) закону України про кримінальну відповідальність; відомості про особу (осіб), місце або річ, щодо яких необхідно провести НСРД; обставини, що дають підстави підозрювати особу у вчиненні злочину; обґрунтування строку проведення зняття інформації з електронних інформаційних систем; обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в інший спосіб; відомості про ідентифікаційні ознаки електронної інформаційної системи; обґрунтування можливості отримання під час проведення цієї НСРД доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин злочину або встановлення осіб, які його вчинили. До клопотання слідчого, прокурора додається витяг з ЄРДР щодо кримінального провадження, у межах якого подається клопотання. 276

В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування. 277

Ідентифікаційними ознаками електронної інформаційної системи є: 278

- 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 ЕОМ.

279 В літературі висловлено пропозицію про те, що зняття інформації з електронних інформаційних систем проводиться у присутності власника, володільця чи утримувача та користувача електронної інформаційної системи і двох понятих, а перед зняттям інформації з електронних інформаційних систем слідчий пред'являє постанову про проведення указаної слідчої дії власнику, володільцю, утримувачу чи користувачу електронної інформаційної системи і пропонує їм відкрити доступ до необхідної для справи інформації[122]. Навряд чи можна погодитися з такою думкою, оскільки такий механізм фактично призводить до втрати цією НСРД її основних ознак, а саме призведе того, що відомості про факти її проведення стануть відомі учасникам кримінального провадження, а отже буде втрачена ознака негласності та конспіративності проведення цієї НСРД.

280 Під час проведення НСРД щодо цифрової інформації збір і аналіз кількісного та якісного складу інформації, яка передається через електронні комунікаційні системи певного комп'ютера, у практичній діяльності можуть бути замінені офіційним вилученням цього комп'ютера та проведенням щодо нього експертизи, оскільки це допоможе отримати інформацію тотожну тій, що перехоплювалась. Однак у такому випадку буде порушено негласність, а для вилучення й тимчасового доступу

[122] *Уваров В. Г.* Зняття інформації з електронних інформаційних систем: новели КПК України та євростандарти. *Форум права*. 2012. № 4. С. 942; *Уваров В. Г.* Втручання у приватне життя шляхом зняття інформації з електронних інформаційних систем: новели нового КПК України та євро стандарти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2012. № 3. С. 443; *Уваров В. Г.* Зняття інформації з електронних інформаційних систем: новели КПК України та євростандарти. *Вісник ХНУВС*. 2012. № 4. Ч. 1. С. 174.

до комп'ютера будуть необхідні процесуальні підстави, тобто ухвала слідчого судді[123].

Всі способи зняття інформації з електронних інформаційних 281
систем можна об'єднати в дві основні групи.

Перша група – це способи безпосереднього доступу. При їх 282
реалізації інформація отримується шляхом видачі відповідних команд з комп'ютера, на якому ця інформація знаходиться.

Друга група охоплює способи опосередкованого 283
(віддаленого) доступу до комп'ютерної інформації.

До них можна віднести: 284

- підключення до лінії зв'язку користувача (наприклад, до телефонної лінії або оптоволоконної лінії) й отримання цим шляхом доступу до електронної інформаційної системи;
- проникнення в комп'ютерну систему за допомогою підбору паролів і т. п.

У протоколі НСРД підлягають відображенню такі відомості: 285
в пам'яті якого пристрою виявлено віртуальні сліди; кому належить пристрій; чи має пристрій вихід у мережу Інтернет, інші електронні комунікаційні або локальні мережі; яка оперативна система функціонує на пристрої (*MacOS, Windows, Linux* – на комп'ютері, *iOS*, *Android*, *HarmonyOS*, *Windows mobile, Symbian* – на 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 НСРД необхідно залучати спеціаліста (програміста, системного адміністратора і т. д.).

---

[123] *Юхно О. О.* Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2. С. 90.

286 Варто погодитися з думкою, що, крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу про проведення НСРД, в ньому бажано фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення:

1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника;
2) серійний номер технічного засобу, 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 представляє 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 НСРД незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації[124];
6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диска комп'ютера,

[124] Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід : монографія. Харків : Право, 2017. С. 159.

необхідно користуватися програмним забезпеченням для побітового копіювання інформації, а після копіювання до протоколу проведення НСРД необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено[125].

287 Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту. Проведення цієї НСРД без дозволу слідчого судді допускається у тому випадку, коли потрібно:

- отримати інформацію, розміщену особою у соціальних мережах, тематичних форумах;
- встановити ідентифікаційні ознаки електронної інформаційної системи за допомогою спеціальних програмних утиліт. Перший їх вид – це утиліти, що надають інформацію про комп'ютери-хости та мережі. Така інформація є необхідною для адресації в мережі і тому є доступною. Другий вид – це утиліти для збору інформації про окремих користувачів, наприклад, реальне ім'я користувача, останній час та дата входження до системи; специфічний вид активності користувача, який увійшов до системи, а інколи навіть поштова адреса та телефон користувача. Однак потрібно пам'ятати, що така інформація може бути несправжньою. Крім того, забороняється використовувати специфічні утиліти, які обходять обмеження, встановлені для користувачів

[1] *Юхно О. О.* Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2. С. 93.

системи. Це, наприклад, різноманітні програми «сніфери», які можна використовувати для перехоплення імен та паролів користувачів[126];
- поспілкуватися з особою за допомогою технології IRC (*Internet Relay Chat*) або *ICQ*;
- ознайомитися з інформацією на робочому комп'ютері працівника, за умови, що користувач не використовує системи логічного захисту інформації (паролі, криптографічні або інші програми захисту інформації).

288 **Аудіо-, відеоконтроль місця.** Відповідно до ст. 270 КПК, аудіо-, відеоконтроль місця як НСРД полягає у здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць без відома їх власника, володільця або присутніх у цьому місці осіб, за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження. Законом ця НСРД віднесена до «інших видів негласних слідчих (розшукових) дій», хоча за своїм характером вона також пов'язана із втручанням у приватне спілкування, оскільки передбачає приховане фіксування відомостей про розмови і поведінку осіб у конкретному місці.

289 Метою зазначеної НСРД є прихована фіксація з використанням аудіо-, відеозаписуючих пристроїв поведінки особи, її розмов або інших рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які відбуваються у публічно доступних місцях, що мають значення для кримінального провадження. Завданням цієї дії є виявлення

[126] Оперативно-розшукова компаративістика : монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. Харків : Золота миля, 2013. С. 283–284.

відомостей, які містять ознаки підготовлюваного, вчинюваного або вчиненого тяжкого або особливо тяжкого злочину.

290 Об'єктом аудіо-, відеоконтролю місця є приватне спілкування особи у публічно доступному місці у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які там відбуваються, зміст яких має значення для досудового розслідування.

291 Суб'єкти проведення аудіо-, відеоконтролю місця аналогічні тим, які проводять аудіо-, відеоконтроль особи.

292 Аудіо-, відеоконтроль місця може проводитись у громадських місцях та в місцях загального користування, доступ до яких необмежений, тобто всередині публічно доступних місць, до яких, відповідно до ч. 2, 3 ст. 267 КПК можна увійти або в яких можна перебувати на правових підставах без відома їх власника, володільця або присутніх у цьому місці осіб. Такими місцями є кінотеатри, ресторани, кафе, музеї тощо.

293 Процесуальний порядок проведення та фіксації цієї НСРД аналогічний аудіо-, відеоконтролю особи.

294 Загалом, аналізуючи аудіо-, відеоконтроль місця як НСРД варто відзначити, що вона є подібною до аудіо-, відеоконтролю особи та спостереженням за особою, річчю або місцем як НСРД. Відрізняються вони місцем їх проведення, організаційно-тактичними особливостями їх здійснення та рівнем технологізації. Як уже зазначалося, законотворці деяких зарубіжних держав, унормовуючи положення процесуальних кодексів, не розмежовують аудіо-, відеоконтроль місця та особи (зокрема, у Республіці Казахстан).

295 Визначаючи особливості аудіо-, відеоконтролю особи, які відрізняють її від спостереження за особою, річчю або місцем, аудіо-, відеоконтролю місця, С. Фомін і С. Гриненко зазначають про те, що вона проводиться щодо конкретної особи як у публічно доступних, так і у публічно недоступних місцях (місцях,

до яких неможливо увійти або в яких неможливо перебувати на правових підставах без отримання на це згоди власника, користувача або уповноважених ними осіб (ч. 2 ст. 267 КПК) чи в умовах, коли учасники спілкування мають достатні підстави вважати, що спілкування є приватним (розумно розраховують на приватність)[127]. Р. Шехавцов і М. Шумило також уважають, що відмінність аудіо-, відеоконтролю особи від передбачених ст.ст. 269, 270 КПК НСРД полягає у використанні аудіо-, відеозаписуючих пристроїв, встановлених усередині публічно недоступних місць для фіксації поведінки особи[128].

296 Також у літературі зазначено, що якщо для візуального спостереження за особою основним завданням є з'ясування і фіксація відомостей щодо її пересування, місць перебування, фактів зустрічей з іншими особами як із застосуванням технічних засобів, так і без, то аудіо-, відеоконтроль особи – НСРД, яка здійснюється з метою отримання інформації і джерелом якої є особа – об'єкт контролю: дії, рухи, висловлювання та інша аудіовізуальна інформація, при цьому місце її знаходження має факультативне значення. Вона проводиться винятково з використанням технічних засобів фіксації інформації[129].

297 Зокрема, Ю. Лисюк зазначає, що нормами КПК передбачається проведення аудіо-, відеоконтролю у двох напрямках, які, на його думку, мають на меті отримання одного й того ж результату, хоча досягають його дещо відмінними

---

[127] 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. 436.

[128] Кримінальний процесуальний кодекс України : наук.-практ. коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. Київ : Юстініан, 2012. С. 574.

[129] 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. 436–437.

способами. Говорячи про відмінність аудіо-, відеоконтролю особи та місця, автор переконує, що єдиною відмінністю цих дій є те, що вони відрізняються місцем їх проведення, тобто здійснюються шляхом установлення СТЗ у публічно доступних місцях, а також інколи в місцях імовірної появи особи. Також особливістю здійснення цих дій є те, що вони відрізняються своїми організаційно-тактичними особливостями, тобто проводяться у громадських місцях і місцях загального користування, доступ до яких не обмежений, і з обов'язковим визначенням в ухвалі слідчого судді повної та точної адреси місця, де проводитиметься НСРД, час і строки її здійснення[130].

298 Отже, особливостями аудіо-, відеоконтролю місця є: 1) проводиться лише у публічно доступних місцях; 2) їх об'єктом є приватне спілкування особи (не конкретної) у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які там відбуваються; 3) організаційно-тактичні особливості проведення.

299 **Тимчасовий доступ до речей та документів.** Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої перебувають такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

300 На підставі аналізу ст. 162 КПК України можна зробити висновок, що найпоширенішою групою електронних доказів є інформація, яка знаходиться в постачальників електронних комунікаційних послуг, про зв'язок, абонента, надання електронних комунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

---

[130] *Лисюк Ю. В.* Аудіо-, відеоконтроль як різновид втручання у приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Науковий вісник Херсонського державного університету*. 2014. Вип. 6–1. Т. 4. С. 79.

301 Також у режимі тимчасового доступу можна отримати доступ до електронних документів, які знаходяться у юридичних та фізичних осіб, зокрема запису камер вуличного спостереження, камер банкоматів тощо. Однак Верховний Суд уважає, що для отримання таких доказів достатньо витребувати їх на підставі запиту слідчого. Так, судді ВС наголосили, що тимчасовий доступ до речей і документів стороні кримінального провадження надається на підставі ухвали слідчого судді місцевого суду під час досудового розслідування чи суду під час судового провадження у випадку, коли в інший спосіб неможливо отримати речі і документи, які можуть мати значення у справі.

302 Як убачається з матеріалів провадження, наявний у справі DVD-R-диск з відеозаписом обставин події з камер відеоспостереження був добровільно наданий директором ТОВ «Р» на запит слідчого, а отже, необхідності звертатися з відповідним клопотанням до слідчого судді для отримання копії цього запису в останнього не було[131].

303 Інформація, що зберігається в постачальників електронних комунікаційних послуг, – це відомості, що виникають під час експлуатації систем мобільного зв'язку як безпосередньо користувачем, а також в операційно-інформаційних системах і центрах комутації операторів мобільного зв'язку. Залежно від місця концентрації, інформація, що зосереджена у засобах систем мобільного зв'язку, міститься: у призначеному для користувача устаткуванні (абонентській станції, абонентському пристрої); різних файлах: текстових, звукових, фото, відео; в операційно-інформаційних системах і центрах комутації оператора стільникового (мобільного) зв'язку (безпосередньо в операторів)[132].

---

[131] Постанова Верховного суду від 10.09.2020 року у справі № 751/6069/19. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/91722819.

[132] *Сербінов О. С.* Окремі види інформації про абонента, яка знаходиться у користуванні операторів мобільного зв'язку та може бути отримана у

Увесь масив інформації про абонента, що зберігається в 304
постачальників електронних комунікаційних послуг, можна поділити на дві групи: перша – відомості стосовно наданих електронних комунікаційних послуг; друга – відомості про споживача, одержані при укладанні договору. До першої групи варто віднести, зокрема: дані про з'єднання терміналів абонентів операторів мобільного зв'язку у певний час («трафіки»), з'єднання певних абонентських номерів або терміналів за певний період часу («звіти»), з'єднання невизначеного кола абонентських номерів (із зазначенням IMEI-терміналу), що відбулись у межах дії певної базової станції за певний період часу («моніторинги») тощо. Відомості про споживача, одержані при укладанні договору – це особисті дані про абонента (копія паспорта, посвідчення водія, службового посвідчення працівника органів державної влади або місцевого самоврядування тощо); реєстраційні дані документів, ідентифікаційний код; відомості стосовно адреси реєстрації, фактичного місця проживання, контактного телефону, адреси електронної пошти тощо[133].

До клопотання слідчий або прокурор повинен також додати: 305

а) відомості (копії довідки оператора, провайдера, протокол допиту, слідчих дій і тощо) про ознаки, які дозволять ідентифікувати абонента шляхом уніфікації мереж (№ SIM карти, IMEI, *e-mail* тощо);

б) копії інших матеріалів, які мають вагоме значення при розгляді клопотання – слідчий суддя, суд при постановленні ухвали в резолютивній частині повинен

ході проведення оперативно-розшукових заходів або слідчих дій. *Адвокат.* 2009. № 1. С. 38.

[133] Використання можливостей операторів стільникового (мобільного) зв'язку для розкриття та розслідування злочинів [Текст] : метод. рекомендації / [Чернявський С. С., Татаров О. Ю., Алексеєва-Процюк Д. О. та ін.]. Київ : Нац. акад. внутр. справ, 2012. С. 15.

зазначати повні дані про особу, щодо якої отримується інформація (прізвище, ім'я, по батькові, місце роботи та ін.);

в) повний номер IMEI, назву оператора, провайдера, номери мобільних станцій, № SIM карти, телефону зі зазначенням коду держави України +38. (Наприклад +38 № SIM-карти телефону; точної електронної адреси мовою оригіналу, із зазначенням знаків розділу; адреси ІА; паролів SIM-карти; номера ICQ; оригінальні назви сайтів; IP-адреси, тощо)[134].

306 Варто погодитися з думкою, що правильною видається практика долучення до клопотання матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів[135].

307 При цьому потрібно враховувати, що радіотехнічна розвідка полягає в установленні постачальниками послуг рухомого зв'язку технічного обладнання, яким охоплюється певна територія або місце. У зв'язку з цим вона не є різновидом втручання в приватне спілкування, а тому проводиться без ухвали слідчого судді[136]. Радіотехнічна розвідка повинна проводитися на підставі доручення на проведення радіотехнічної розвідки

---

[134] *Тагієв С. Р.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 21.

[135] *Ткачик А. Б.* Таємниця спілкування та її обмеження в кримінальному провадженні : дис. … д-ра філос. за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 – Право). Львівський державний університет внутрішніх справ, Львів, 2021. С. 107.

[136] Постанова Верховного суду від 16.03.2021 р. у справі № 364/673/18. URL : https://ips.ligazakon.net/document/c017923?an=&ed=&dtm=&le=.

виданого слідчим чи прокурором на підставі п. 3 ч. 2 ст. 40 КПК відповідному оперативному підрозділу.

308 У разі задоволення клопотання ухвала слідчого судді про надання тимчасового доступу до речей і/або документів повинна містити чітку вказівку на те:

- хто повинен надати тимчасовий доступ до речей і документів (із зазначенням повної та точної назви юридичної особи її юридичної адреси;
- якщо вказаний обов'язок покладено на фізичну особу, то зазначається її прізвище, ім'я та по батькові);
- кому повинно бути надано тимчасовий доступ до речей і документів (із зазначенням прізвища, імені, по батькові, а також посади уповноваженої особи);
- які саме необхідно надати документи для ознайомлення, отримання їх копій чи здійснення виїмки;
- який строк встановлено для застосування вказаного заходу[137].

309 Ураховуючи специфіку формату зберігання інформації, що передбачена п. 7 ч. 1 ст. 162 КПК України і знаходиться в постачальників електронних комунікаційних послуг, надання доступу до відповідних документів (тобто надання можливості ознайомитися з ними та зробити з них копії), може відбуватися як безпосередньо в оператора (провайдера), так і шляхом надання доступу до відповідних документів уповноваженому на зняття інформації з електронних комунікаційних мереж підрозділу правоохоронного органу через відповідні інформаційні системи відповідно до встановленого порядку з обов'язковим наданням копії ухвали слідчого судді відповідному оператору (провайдеру)[138].

---

[137] *Сліпченко В. І.* Тимчасовий доступ до речей і документів: процесуальний порядок отримання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2013. № 2. С. 512.

[138] *Алєксєєва-Процюк Д. О., Брисковська О. М.* Особливості проведення тимчасового доступу до речей та документів для отримання інформації від операторів мобільного зв'язку. *Митна справа*. 2013. № 1. С. 58–65.

310 Одержання (вилучення) інформації безпосередньо в постачальників електронних комунікаційних послуг вимагає забезпечення участі у проведенні цього заходу спеціалістів, передусім фахівців у галузі комп'ютерних технологій, засобів зв'язку або обслуговування мережі. Вилучення електронних комунікаційних повідомлень здійснюється у присутності представника оператора мобільного зв'язку, понятих (бажано з числа працівників фірми-оператора). Залежно від змісту повідомлень, вони можуть бути вилучені шляхом копіювання вмісту на магнітні носії комп'ютерної інформації (у цьому разі ще на підготовчій стадії вилучення необхідно підготувати апаратно-технічні засоби для зчитування і збереження інформації, що вилучається, перелік яких варто попередньо узгодити зі спеціалістом, а також переносні накопичувальні пристрої)[139].

311 **Отримання електронних доказів від учасників кримінального провадження.** Верховний Суд правильно дійшов висновку, що добровільне надання свідком стороні обвинувачення диска з відеозаписом ДТП, що було підтверджено ним у судовому провадженні, а не отримання його на підставі тимчасового доступу до речей і документів, не є підставою для визнання такого доказу недопустимим. Диск як матеріальний носій є способом збереження інформації з електронного документа і вважається його оригіналом, а тому є належним та допустимим доказом у кримінальному провадженні.

312 При цьому суд керувався такими міркуваннями. Відповідно до приписів частин 1, 2 ст. 93 КПК, збирання доказів здійснюється сторонами кримінального провадження у порядку, передбаченому цим Кодексом. Сторона обвинувачення

---

[139] *Чернявський С. С., Фінагеєв В. О.* Проблеми тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 183.

здійснює збирання доказів шляхом як проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, так і витребування та *отримання* від органів державної влади, місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених КПК.

313 Наведеними кримінальними процесуальними нормами встановлено порядок отримання стороною обвинувачення від особи за її ініціативою і доброю волею, диска з відеозаписом із відеореєстратора, наданого за її письмовою заявою на ім'я слідчого, що свідок підтвердила в судовому провадженні.

314 При цьому необхідно зважати на те, що згідно з ч. 4 ст. 132 КПК, для оцінки потреб досудового розслідування варто враховувати можливість отримати речі й документи, які можуть бути використані під час судового розгляду для встановлення обставин у кримінальному провадженні, без застосування заходу забезпечення кримінального провадження.

315 Отримання тимчасового доступу до речей, документів і, за наявності підстав для того, розпорядження про надання можливості вилучення речей і документів, обумовлене, за приписами ст. 163 КПК, необхідністю доведення стороною кримінального провадження наявності достатніх підстав уважати, що без такого доступу та вилучення існує реальна загроза зміни або знищення речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів.

316 За відсутності таких обставин, тим більше за умови добровільного надання документів стороною чи учасником кримінального провадження, у володінні яких вони перебувають, не виникає підстав та умов до звернення з клопотанням до слідчого судді стосовно застосування заходів забезпечення

кримінального провадження у вигляді тимчасового доступу до документів і речей[140].

317 Аналогічну позицію висловив Верховний Суд в іншій аналогічній справі. Зокрема, він вказав, що збирання та подання доказів у кримінальному провадженні є різними способами одержання доказової інформації з огляду на їх відмінну правову природу, а саме збирання доказів відбувається через інститут слідчих дій, а подання доказів здійснюється особою добровільно шляхом передачі слідчому, прокурору предметів або документів, які, на її думку, мають значення для кримінального провадження. Під час отримання предметів та документів, представлених особою для залучення їх до справи як докази, орган дізнання, слідчий або суд повинні допитати цю особу з метою з'ясування джерела та обставин їх отримання, потім здійснити огляд цих предметів або документів і процесуально зафіксувати їх отримання.

318 Як вбачається з матеріалів кримінального провадження, свідок добровільно та за власною ініціативою надав слідчому зазначений диск з відеозаписом з камер відеоспостереження. Зазначений факт свідок підтвердив під час його допиту в суді першої інстанції.

319 Тож, надання цього диска з відеозаписом безпосередньо свідком, не можна вважати порушенням вимог ст. 93 КПК, оскільки сторона обвинувачення здійснює збирання доказів шляхом, у тому числі, отримання від фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом[141].

---

[140] Постанова Верховного суду від 31.03.2021 р. у справі № 333/1539/16-к. URL : https://ips.ligazakon.net/document/c018510?an=88

[141] Постанова Верховного суду від 19.05.2021 р. у справі № 204/4521/18. URL : https://ips.ligazakon.net/document/c018840

Відповіді на запитання кейсів

КЕЙС 1. *В описаній ситуації доцільно провести комплекс НСРД, спрямованих на встановлення особи підозрюваного та отримання необхідної доказової інформації про обставини вчиненого кримінального правопорушення.*

Зокрема, потрібно провести:

- *зняття інформації з електронних комунікаційних мереж, використовуючи ідентифікуючі ознаки: номер мобільного телефону (050-721-66-92) та електронну адресу – ivan@mail.ru;*
- *за можливості зняття інформації з електронної інформаційної системи мобільного терміналу з номером (050-721-66-92).*

КЕЙС 2. *В описаній ситуації необхідно провести судову комп'ютерно-технічну експертизу, предметом якої виступатимуть: а) комп'ютерна техніка; б) мобільні телефони. Доручити проведення відповідної експертизи треба експертам НДЕКЦ або НДІСЕ.*

Орієнтовні питання комп'ютерно-технічної експертизи телефона:

Які контакти та їх номери містяться на мобільному телефоні марки "..." IMEI ..., та сім-карті стільникового зв'язку "...", яка в ньому знаходиться?

Дзвінки на які номери мобільних операторів здійснено та з яких номерів мобільних операторів отримувались дзвінки із зазначенням дати та часу з мобільного телефону, із сім-карткою стільникового зв'язку, яка в ньому знаходиться?

Які повідомлення містяться, на які номери мобільних операторів вони відправлялись та з яких отримані із зазначенням дати та часу з мобільного телефону, із сім-карткою стільникового зв'язку, яка в ньому знаходиться?

Чи містяться в наданому на дослідження мобільному телефоні "..." IMEI ... з карткою мобільного оператора за номером ..., який належить ... програма "..."?

Під якими обліковим записом, псевдонімом, номером телефону у вказаній програмі зареєстрований власник мобільного телефону?

Які переписки містяться у програмі "..."?
Яка інформація про дзвінки та СМС-повідомлення міститься у пам'яті телефону?
Чи міститься у пам'яті телефону зображення?

Орієнтовні питання комп'ютерно-технічної експертизи комп'ютерної техніки:
Чи є пристрої (системні блоки "..." в кількості ... шт.), надані для проведення експертизи, у працездатному стані?
До якого типу належать надані для проведення експертизи пристрої?
Чи є пристрої, надані для проведення експертизи, виготовленими заводським способом, і хто їх виробник?
Яке програмне забезпечення міститься та використовувалось на наданих для дослідження пристроях, та яке функціональне призначення цього програмного забезпечення?
Які інтернет-ресурси відвідували з наданих на дослідження пристроїв?
Чи містяться на наданих для дослідження пристроях програмні налаштування для підключення до зовнішніх серверів, якщо так, то до яких саме?
Чи можливе використання пристроїв, наданих для проведення експертизи, в якості пристроїв для проведення азартних ігор для отримання виграшу?

Запитання для самоконтролю

1. Якими унікальними особливостями характеризується інформація, створена за допомогою високих інформаційних технологій?
2. На яких рівнях функціонує інформація в ЕОМ?
3. Які особливості перевірки цифрового алібі?
4. Яким умовам повинна відповідати виявлена помилка програмного забезпечення?
5. Які основні методи фіксації інформації з веб-сайту?
6. Розмежуйте поняття електронного доказу та його носія.
7. Чи є поняття електронного документа та електронного доказу тотожними?

8. У чому суть належності електронного доказу як його юридичної властивості?

9. У чому суть допустимості електронного доказу як його юридичної властивості?

10. У чому суть достовірності електронного доказу як його юридичної властивості?

11. Чи впливає відсутність кваліфікованого електронного підпису електронного документа на достовірність певних даних в електронній формі та їх доказове значення?

12. У чому суть «принципу недискримінації при дослідженні електронних доказів»?

13. Поясність зміст презумпції цілісності (достовірності) електронних доказів.

14. Чи застосовним до електронних доказів є принцип самоідентифікації автора?

15. Які можна виокремити способи перевірки та оцінки електронних доказів?

16. Які підстави проведення аудіо-, відеоконтролю особи?

17. Які завдання проведення аудіо-, відеоконтролю особи?

18. Що потрібно розуміти під електронною комунікаційною мережею?

19. На кого покладається обов'язок зняття інформації з електронних комунікаційних мереж?

20. Які ідентифікаційні ознаки електронних комунікаційних мереж повинні бути зазначені в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування?

21. Що потрібно розуміти під електронною інформаційною системою?

22. На які види можна поділити електронні інформаційні системи за архітектурою?

23. У яких випадках не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем?

24. Що потрібно розуміти під подоланням системи логічного захисту електронної інформаційної системи?

25. Які ідентифікаційні ознаки електронної інформаційної системи повинні бути зазначені в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування?

26. Які засоби захисту інформації, отриманої в результаті НСРД, передбачає законодавець?

27. Розмежуйте зняття інформації з електронних інформаційних систем та тимчасовий доступ до відомостей, що у них містяться.

28. Чи допускається проведення описаних у розділі НСРД у кримінальних провадженнях щодо кримінальних проступків?

29. Чи допускається проведення описаних у розділі НСРД до внесення відомостей до ЄРДР?

30. Якими ще слідчими (розшуковими) чи іншими процесуальними діями можна одержати електронні докази?

Рекомендована література

1. *Багрій М. В., Луцик В. В.* Негласні слідчі (розшукові) дії у кримінальному провадженні : монографія. Тернопіль, 2014. 308 с.

2. *Багрій М. В., Луцик В. В.* Процесуальні аспекти негласного отримання інформації : вітчизняний та зарубіжний досвід : монографія. Харків : Право, 2017. 376 с.

3. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навчально-практичний посібник / Б. І. Бараненко, О. В. Бочковий, К. А. Гусєва та ін. ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

4. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

5. *Марущак А. І.* Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104–110.

6. Негласні слідчі (розшукові дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні : навч.-практ. посібник [Текст] / Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Харків : Оберіг, 2015. 424 с.

7. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рекомендації / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

8. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рекомендації / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

9. *Тагієв С. Р.* Негласні слідчі (розшукові) дії у кримінальному судочинстві України : монографія [Текст]. Київ : ВД «Дакор», 2015. 440 с.

10. *Тарасюк А. В.* Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. 192 с.

11. *Cascavilla G., Tamburri D. A., Van Den Heuvel W.-J.* Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & security. 2021. Vol. 105. P.102258.

12. *Edwards G.* Cybercrimes Investigators Handbook. Hoboken, New Jersey: John Wiley & Sons, Incorporated. 2020. 297 p.

13. *Tropina T., Callanan C.* Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing AG Switzerland, 2015.

ЗМІСТ

Умовні позначення **7**

Про проєкт **9**

Передмова **12**

Розділ 1. Кіберзлочинність: поняття, види та запобігання **14**

1.1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів (*О. Денькович*) 14

1.2. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система (*О. Денькович*) 37

1.3. Детермінанти та основні напрями запобігання кіберзлочинності (*Б. Головкін*) 47

Розділ 2. Особливості методики розслідування кіберзлочинів (*Д. Цехан*) 88

Розділ 3. Електронні докази у кримінальному провадженні **122**

3.1. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види (*Д. Цехан*) 122

3.2. Способи збирання електронних доказів *(В. Луцик)* 140

Додатки **199**

Список використаних джерел **279**

Предметний покажчик **294**

Про авторів **296**

CRIM HUM

Co-funded by the Erasmus+ Programme of the European Union

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ



Посібник

598471-EPP-1-2018-1-AT-EPPKA2-CBHE-JP

Modernising Master's Training on Criminal Justice
CRIMHUM

CYBERCRIME AND DIGITAL EVIDENCE

Lviv
Ivan Franko National University of Lviv
2022

Authors:
Bohdan Holovkin, Olha Denkovych, Vasyl Lutsyk, Dmytro Tsekhan

Edited by:
Olha Denkovych, Gabriele Schmölzer

Удосконалення магістерської програми
з кримінальної юстиції

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ

Навчальний посібник

За редакцією
кандидата юридичних наук, доцента Ольги ДЕНЬКОВИЧ,
доктора права, професора Габріеле ШМЕЛЬЦЕР

Львів
ЛНУ ім. Івана Франка
2022

УДК [343.3/7:004](075.8)
К 39

Автори:
Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан

Рецензенти:
Олексій Гумін, доктор юридичних наук, професор,
завідувач кафедри кримінального права і процесу Національного
університету «Львівська політехніка»,
Тарас Созанський, кандидат юридичних наук, професор,
перший проректор Львівського державного університету
внутрішніх справ

Серія заснована в 2020 році

Видання підготовлено в рамках проєкту Програми Європейського Союзу ERASMUS+ «Модернізація магістерських програм для майбутніх суддів, прокурорів, слідчих з урахуванням європейських стандартів у сфері прав людини» (598471-EPP-1-2018-1-AT-EPPKA2-CBHI-JP), керівниця проєкту – *Габріеле Шмельцер*

К 39 **Кіберзлочинність та електронні докази** = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с. – (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

ISBN 978-617-10-0805-2 (серія)
ISBN 978-617-10-0807-6 (електрон. вид.)

У навчальному посібнику розглянуто поняття кіберзлочину та кіберзлочинності, особливості запобігання кіберзлочинності, особливості методики розслідування цієї категорії кримінальних правопорушень. Окрему увагу приділено поняттю та особливостям електронних доказів, способам їх збирання та правильного процесуального оформлення результатів процесуальних дій, спрямованих на їх збирання.

Нормативну базу і правозастосовну практику в посібнику проаналізовано станом на 1 жовтня 2022 року.

Навчальний посібник призначений для магістрів, що навчаються за спеціальністю 081 «Право».

УДК [343.3/7:004](075.8)

ISBN 978-617-10-0805-2 (серія)
ISBN 978-617-10-0807-6 (електрон. вид.)

© Головкін Б. М., Денькович О. І.,
Луцик В. В., Цехан Д. М., 2022

ПРО АВТОРІВ



Головкін Богдан Миколайович
(*розділ 1, підрозділ 1.3*)
Завідувач кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, доктор юридичних наук, професор.
Сфера наукових інтересів: теорія кримінології, боротьба з економічною, організованою та кіберзлочинністю, протидія корупції, віктимологія.



Денькович Ольга Іванівна
(*розділ 1, підрозділи 1.1, 1.2*)
Доцент кафедри кримінального права і кримінології юридичного факультету Львівського національного університету імені Івана Франка, кандидат юридичних наук, доцент.
Сфера наукових інтересів: питання кримінального права, зокрема принципів кримінального права та кримінально-правових ризиків здійснення господарської діяльності; міжнародне кримінальне право; міжнародні стандарти кримінально-правової охорони прав людини, практика Європейського Суду з прав людини з питань кримінального права і процесу.



Луцик Василь Васильович
(*розділ 3, підрозділ 3.2*)
Доцент кафедри кримінального процесу та криміналістики факультету Львівського національного університету імені Івана Франка, кандидат юридичних наук, доцент.
Сфера наукових інтересів: негласні слідчі (розшукові) дії, прокурорське право, порівняльний кримінальний процес.



Цехан Дмитро Миколайович
(*розділ 2, розділ 3, підрозділ 3.1*)
доцент кафедри криміналістики Національного університету "Одеська юридична академія", кандидат юридичних наук, доцент
Сфера наукових інтересів: доказування у кримінальному провадженні; цифрові докази; використання високих інформаційних технологій у протидії злочинності; пенітенціарна злочинність; оперативно-розшукова діяльність в установах виконання покарань.

Електронне навчальне видання

Удосконалення магістерської програми з кримінальної юстиції

Головкін Богдан Миколайович,
Денькович Ольга Іванівна,
Луцик Василь Васильович,
Цехан Дмитро Миколайович

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ

Навчальний посібник

За редакцією
кандидата юридичних наук, доцента Ольги ДЕНЬКОВИЧ,
доктора права, професора Габріеле ШМЕЛЬЦЕР

Редактор *Уляна Крук*
Комп'ютерне верстання *Світлани Сеник*

Формат 60x84/$_{16}$. Ум. друк. арк. 17,32. Тираж 300 пр. Зам.

Видавець та виготовлювач:
Львівський національний університет імені Івана Франка
вул. Університетська, 1, м. Львів, 79000.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції.
Серія ДК № 3059 від 13.12.2007 р.