в тому, що слідчий, прокурор починає одночасний допит двох чи більше вже допитаних осіб із з'ясування менш істотних спірних обставин, але поступово все більше і більше їх загострює. У такій обстановці особа всупереч своєму бажанню переходить від обговорення менш важливих спірних питань до більш важливих [2, с. 168].

8. Зміна черговості постановки питань. У процесі одночасного допиту двох чи більше раніше допитаних осіб слідчий повинен уважно слідкувати за змістом відповідей кожного з допитуваних. Якщо один з учасників слідчої (розшукової) дії здійснює спроби узгодити свої показання з іншим учасником, слід змінювати черговість постановки запитань. Цей тактичний прийом дозволяє викрити брехню несумлінного учасника і перешкоджає змові допитуваних [2, с. 171].

Таким чином, одночасний допит двох або більше раніше допитаних осіб, як правило відбувається за умов конфліктної ситуації. Додатково процес його проведення між учасниками ОЗГ ускладнюється безпосередньо їх соціальними статусами, кримінальними характеристиками та психологічними особливостями, а також наявністю певного «професійного» злочинного досвіду, що може призвети до використання допитуваними зазначеної СРД у власних цілях, з метою узгодження показань та координації лінії поведінки під час розслідування.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

2. Жалдак І. А. Тактика одночасного допиту двох чи більше вже допитаних осіб : дис. … канд. юрид. наук : 12.00.09. Київ, 2019. 240 с.

3. Плосконос А. І. Організаційно-тактичні заходи підготовки до допиту учасників організованих злочинних груп та злочинних організацій. KELM: Knowledge, Education, Law, Management. 2018. №2 (22). С. 152-157.

4. Плосконос А. І. Тактичні прийоми допиту учасників організованих злочинних груп та злочинних організацій. Підприємництво, господарство і право. № 11. Київ, 2020. С.260-265.

Самодін Артем Володимирович,
завідувач кафедри криміналістики
та судової медицини Національної академії
внутрішніх справ, кандидат юридичних
наук, доцент

СУЧАСНЕ РОЗУМІННЯ ФЕНОМЕНУ «ЦИФРОВА КРИМІНАЛІСТИКА»

Одним із сучасних викликів для України у сфері кібербезпеки є змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету

речей, штучного інтелекту тощо [9]. Адже сучасні тенденції розвитку «цифровізації (диджитиза́ції)» майже усіх сфер суспільних відносин в нашій країні створюють передумови для більш ґрунтовної розробки цих напрямів у юридичних науках.

Не є й виключенням й криміналістика, адже в інформаційному просторі з'явились та досить широко та, подекуди не зовсім обґрунтовано, використовується як окремі узагальнені поняття «цифрова криміналістика», «комп'ютерна криміналістика», «мобільна криміналістика», «відеокриміналістика». Найбільш вживаним, як нами відмічається, є словосполучення «цифрова криміналістика». Такий стан речей обумовлений перш за все не повним розумінням окремих спеціалістів-практиків у сфері ІТ-технологій розуміння самого предмету, завдань та системи криміналістики як науки та галузі юридичних знань.

Зважаючи на саме поняття криміналістики як науки про закономірності механізму кримінального правопорушення, виникнення інформації про кримінальне правопорушення та його учасників, закономірності збирання, дослідження, оцінки та використання доказів, та заснованих на пізнанні цих закономірностей спеціальних засобах і методах досудового розслідування, судового розгляду і попередження кримінальних правопорушень [1, с. 31], а також її чотирьох елементну систему до якої традиційно входять: загальна теорія криміналістики, криміналістична техніка, тактика та методика, самостійне існування поняття як «цифрова криміналістика» викликає чимало запитань щодо його розуміння як певного наукового та прикладного феномену.

Зокрема в окремих інформаційних джерелах, у тому числі у науковій літературі, зазначене поняття визначається як нові знання у криміналістиці, які базуються на розумінні особливостей функціонування сучасних інформаційно комунікаційних технологій і використовуються для розкриття та розслідування кримінальних правопорушень та має синоніми «електронна криміналістика» і «комп'ютерна криміналістика» (Яковлев О.М.) [2].

Досить цікавим, є розуміння цього феномену Федотовим М.М., який визначає «Форензіку – Комп'ютерну криміналістику» як прикладну науки щодо розкриття та розслідування злочинів, які пов'язані з комп'ютерною інформацією, методів отримання та дослідження доказів, що мають форму комп'ютерної інформації (так званих цифрових доказів), технічних засобів, які застосовуються для цього. А до її предметів відносить: кримінальну практику; оперативну, слідчу та судову практику щодо комп'ютерних злочинів; методи експертного дослідження комп'ютерної інформації; здобутки галузей зв'язку та інформаційних технологій [6, с. 12–13] (авт. переклад з російської мови).

«Цифрова криміналістика» у різних формулюваннях вже досить тривалий час зустрічається під час аналізу певних освітньо-професійних програм підготовки на бакалаврському та магістерському рівнях. Зокрема, у Харківському національному університеті імені

В.Н. Каразіна за спеціальністю 125 «Кібербезпека» на першому бакалаврському рівні викладається навчальна дисципліна «Основи протидії кіберзлочинності та цифрова криміналістика» [7]. Наприклад, в контексті навчальної дисципліни «Цифрова криміналістика», яка викладається у Харківському національному економічному університеті імені Семена Кузенця для згідно з навчальним планом підготовки фахівців другого освітнього рівня «магістр» спеціальності 125 «Кібербезпека», комп'ютерна криміналістика (computer forensics), у ширшому сенсі цифрова криміналістика (digital forensics) визначається як підрозділ криміналістики, прикладна наука про розслідування злочинів (інцидентів) та збирання цифрових доказів, що знаходяться на комп'ютерах, системах зберігання даних, у комп'ютерних мережах, на мобільних й інших цифрових пристроях (авт. переклад з російської мови). При цьому, вже предметом цієї навчальної дисципліни автори визначають основні поняття та методи цифрової криміналістики, навики збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux [3].

У профільних закладах вищої освіти зі специфічними умовами навчання, наприклад, у Харківському національному університеті внутрішніх справ за цією ж спеціальністю курсанти вивчають «Цифрову криміналістику», у якій розглядаються теми присвячені електронним (цифровим) доказам, процес первинних цифрових криміналістичних досліджень, структура жорсткого диску та файлових систем, здобуття даних та створення дублікатів носіїв даних, подолання протидії криміналістичним дослідженням та їх певні напрями, наприклад: операційних систем, комп'ютерних мереж, веб-атак, баз даних, хмарних сервісів, шкідливого програмного забезпечення, електронної пошти, мобільних пристроїв, а також складання звіту і представлення їхніх результатів [8].

Окремі спеціалісти у сфері ІТ-технологій, зокрема, Української академії кібербезпеки, використовують, на наш погляд, загальновживане узагальнене формулювання «цифрова криміналістика», визначаючи її завданням збирання, обробку, зберігання, аналіз та надсилання доказів, пов'язаних з комп'ютерною технікою, для пом'якшення наслідків уразливості мережі та/або для кримінальних, шахрайських, контррозвідувальних або правоохоронних розслідувань [4]. Спеціалісти Лабораторії комп'ютерної криміналістики, визначають певну сферу «комп'ютерної криміналістики» до якої, як комерційні послуги, відносять: експертизи та дослідження (комп'ютерно-технічні експертизи та криміналістичні дослідження цифрової техніки); збір цифрових доказів (у тому числі технічний супровід слідчих дій (оглядів, обшуків); мобільна криміналістика (наприклад, вилучення і аналіз усіх даних (переписки, медіа, документів та ін.) з сучасних мобільних пристроїв); відео криміналістика (наприклад, знімання і відновлення даних з усіх типів відеореєстраторів).

Зі врахуванням викладеного, як самостійне формулювання «цифрова криміналістика» або ж її споріднені інтерпретації доцільно використовувати та розглядати виключно в контексті окремих навчальних дисциплін як певну сукупність міжпредметних знань, яких мають набути здобувачі вищої освіти для успішного виконання завдань майбутньої професійної діяльності у межах спеціалізації, а в окремих випадках як напрям та форму надання відповідних комерційних послуг у сфері цифрових технологій.

Водночас, з огляду на предмет науки криміналістики, й зокрема самостійної прикладної юридичної навчальної дисципліни, яка викладається на її основі, знання про цифрові технології мають знаходити свій вияв у контексті:

– криміналістичної техніки (наприклад, використання технологій аналізу «великих даних» (англ. Big Data) в розрізі напряму інформаційно-довідкового забезпечення правоохоронної діяльності (криміналістична реєстрація), використання дакто-сканерів в дактилоскопії, програм призначених для обробки цифрових зображень з технічних засобів фотофіксації безпілотних літальних апаратів у криміналістичній фотографії тощо);

– криміналістичної тактики (наприклад, використання під час організації та планування розслідування інформаційних систем кримінального аналізу та розвідувальної аналітики; тактичних особливостей проведення допиту та впізнання у режимі відеоконференції під час досудового розслідування; використання спеціальних знань та залучення спеціалістів у сфері ІТ-технологій до проведення огляду, обшуку з метою надання консультативної допомоги слідчому у роботі зі цифровими доказами та їх носіями; призначення та проведення комп'ютерно-технічних експертиз тощо);

– криміналістичної методики щодо розслідування не лише кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а й інших кримінальних правопорушень у методиці розслідування, яких звертається увага на аналіз цифрових даних відносно способу і засобів їх вчинення, доцільності, а подекуди й необхідності використання можливостей сучасних досягнень у сфері інформаційних технологій під час їх розслідування.

Варто констатувати, що окреслений нами напрям безсумнівно має досліджуватись на науковому та навчально-методичному рівнях не лише з позиції криміналістики, а й інших споріднених юридичних наук, при цьому напрацювання мають ефективно впроваджуватись у слідчу, судово-експертну практику та підготовку здобувачів вищої освіти.

Список використаних джерел

1. Криміналістика : підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. Самодін та ін.] ; за заг. ред. В. В. Пясковського. 2-ге вид., перероб. і допов. Харків : Право, 2020. 752 с.

2. Заєць І.С. Перспективи криміналістики в умовах інформатизації суспільства. Електронний репозитарій Національної академії внутрішніх справ. URL: http://elar.naiau.kiev.ua.
3. Компьютерная криминалистика в Украине. Проблемы и пути развития. URL: https://pns.hneu.edu.ua/course/view.php?id=5683.
4. Українська академія кібербезпеки. Веб-сайт. URL: https://uacs.kiev.ua/workforce-roles-framework/tsyfrova-kryminalistyka/
5. Лабораторія комп'ютерної криміналістики. Веб-сайт. URL : https://cyberlab.com.ua/index.html
6. Федотов Н.Н. Форензика – компьютерная криминалистика. Москва : Юридический Мир, 2007. 432 с.
7. Освітньо-професійна програма «Кібрербезпека у фінансових технологіях». Веб-портал Харківського національного університету імені В.Н. Каразіана. URL: http://start.karazin.ua/app/webroot/files/upload/2021/kbi/b-iberbezpeka.pdf.
8. Освітньо-професійна програма «Кібрербезпека (поліцейські)». URL: http://univd.edu.ua/files/125_cyber/opp_125_2020.pdf.
9. Стратегія кібербезпеки України «Безпечний кіберпростір - запорука успішного розвитку країни». Указ Президента України від 26 серп. 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text.

Свобода Євгенія Юріївна,
професор кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ, кандидат юридичних наук, доцент;
Михальчук Тетяна Володимирівна,
старший викладач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ, кандидат юридичних наук

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ВІДЕОРЕЄСТРАТОРІВ ПІД ЧАС ПОРУШЕННЯ ПРАВИЛ ДОРОЖНЬОГО РУХУ

Відеореєстратор (англ. digital video recorder, DVR) – пристрій, призначений для запису, зберігання та відтворення відеоінформації.

Відеореєстратори, в основному, використовуються у системах відеоспостереження як стаціонарних (на об'єктах), так і рухомих (наприклад, автомобільні відеореєстратори).

В залежності від поставлених завдань відеореєстратор може використовуватися для:

– відеоспостереження за відвідувачами в приватних будинках, офісах, магазинах;